

BERNSTEIN LITOWITZ BERGER  
& GROSSMANN LLP  
DAVID R. STICKNEY (Bar No. 188574)  
(davids@blbglaw.com)  
RICHARD D. GLUCK (Bar No. 151675)  
(rich.gluck@blbglaw.com)  
LUCAS E. GILMORE (Bar No. 250893)  
(lucas.gilmore@blbglaw.com)  
12481 High Bluff Drive, Suite 300  
San Diego, CA 92130  
Tel: (858) 793-0070  
Fax: (858) 793-0323

-and-

AVI JOSEFSON  
(avi@blbglaw.com)  
1251 Avenue of the Americas  
New York, NY 10019  
Tel: (212) 554-1400  
Fax: (212) 554-1444

*Attorneys for Lead Plaintiff Louisiana Sheriffs'  
Pension & Relief Fund and Lead Counsel for the Class*

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

IN RE INTEL CORPORATION  
SECURITIES LITIGATION

Master Case No. 18-cv-00507-YGR

ECF CASE

**CONSOLIDATED CLASS  
ACTION COMPLAINT FOR  
VIOLATIONS OF THE  
FEDERAL SECURITIES LAWS**

DEMAND FOR JURY TRIAL

## **TABLE OF CONTENTS**

	<u>Page</u>
I. INTRODUCTION .....	1
II. JURISDICTION AND VENUE.....	5
III. PARTIES .....	5
A. Plaintiff.....	5
B. Defendants.....	5
IV. SUMMARY OF THE FRAUD .....	9
A. Intel, Its Products And Operating Groups .....	9
B. Intel’s Quest To Develop Faster, More Powerful Processors .....	13
C. Intel Assures Customers That Its Processors Provide Security .....	16
D. Intel’s Processors Sacrificed Security For Performance .....	17
E. Google Engineers Discover Flaws In Intel’s Processors .....	17
F. Google Analysts Tell Intel About Spectre And Meltdown On June 1, 2017.....	19
G. Intel’s Obstacles To Fixing Or Mitigating The Security Defects.....	22
H. Intel Confirms Google Project Zero’s Findings.....	23
I. Defendants Continued To Promote Security And Performance, While Concealing Spectre And Meltdown .....	28
J. Krzanich’s Insider Trading.....	36
K. The Truth Emerges Through A Series Of Partial Disclosures.....	39
L. Patches Are Ineffective .....	44
V. DEFENDANTS’ FALSE AND MISLEADING STATEMENTS AND OMISSIONS.....	46
A. Statements On Intel’s Website .....	46
B. October 26, 2017 3-Q 2017 Results .....	57
C. October 27, 2017 Intel Publication - Unlocking Data Insights With The Powerful Intel Xeon Scalable Processor.....	58
D. November 14, 2017 UBS Global Technology Conference.....	59

1	E.	November 28, 2017 Credit Suisse Technology, Media And Telecom Conference.....	60
2	F.	December 5, 2017 Intel Corp At Nasdaq Investor Program .....	61
3	G.	December 20, 2017 Intel Hardware-Based Security Video .....	62
4	VI.	ADDITIONAL ALLEGATIONS OF DEFENDANTS’ SCIENTER .....	63
5	VII.	LOSS CAUSATION .....	66
6	VIII.	PRESUMPTION OF RELIANCE .....	67
7	IX.	DEFENDANTS’ DUTY TO DISCLOSE.....	68
8	X.	INAPPLICABILITY OF THE STATUTORY SAFE HARBOR AND BESPEAKS CAUTION DOCTRINE .....	69
9	XI.	CLASS ACTION ALLEGATIONS.....	70
10	XII.	CLAIMS FOR RELIEF .....	71
11	COUNT I	For Violations Of Section 10(b) Of The Exchange Act And SEC Rule 10b-5 Promulgated Thereunder (Against All Defendants).....	71
12	COUNT II	For Violation Of Section 20(a) Of The Exchange Act Against Defendants Krzanich, Swan And Shenoy .....	73
13	XIII.	PRAYER FOR RELIEF .....	74
14	XIV.	JURY DEMAND.....	75
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			

1           Lead Plaintiff Louisiana Sheriffs’ Pension & Relief Fund (“Louisiana Sheriffs” or  
2 “Lead Plaintiff”), by and through its counsel, alleges the following based upon personal  
3 knowledge as to itself and its own acts and upon information and belief as to all other  
4 matters. Lead Plaintiff’s information and belief is based on the ongoing independent  
5 investigation of its undersigned counsel. This investigation includes review and analysis  
6 of: (i) Intel Corporation’s (“Intel” or the “Company”) public filings with the U.S. Securities  
7 and Exchange Commission (“SEC”); (ii) research reports from securities and financial  
8 analysts; (iii) videos and transcripts of Intel’s conference calls and presentations to analysts  
9 and investors; (iv) Company press releases and reports; (v) Company website and  
10 marketing materials; (vi) news and media reports concerning the Company and other facts  
11 related to this action; (vii) pleadings and additional materials from cases against Intel  
12 arising from Spectre and Meltdown in the multidistrict litigation entitled *In re Intel*  
13 *Corporation CPU Marketing, Sales Practices and Products Liability Litigation*, 18-md-  
14 02828-SI (D. Or.); (viii) price and volume data for Intel securities; (ix) consultation with  
15 relevant experts; (x) accounts from former Intel employees; and (xi) additional materials  
16 and data concerning the Company and industry as identified herein.

## 17 **I. INTRODUCTION**

18           1. This securities class action arises from Defendants’ false and misleading  
19 statements and omissions about the security and performance of Intel’s processors, while  
20 concealing the existence of structural flaws – known as Spectre and Meltdown – that create  
21 security threats exposing passwords, encrypted communications and all manner of  
22 sensitive information to hackers. Defendants’ misrepresentations inflated the price of  
23 Intel’s common stock until a series of partial disclosures caused the stock price to fall.  
24 Lead Plaintiff brings this action under Sections 10(b) and 20(a) of the Securities Exchange  
25 Act of 1934 on behalf of purchasers of Intel common stock between October 27, 2017 and  
26 January 9, 2018 (the “Class Period”).

27           2. Intel is one of the world’s largest manufacturers of processors, chipsets, and  
28 related computer components. Intel provides processors to more than 90 percent of all

1 personal computers and servers supporting the internet and business operations. Intel  
2 markets its products as faster, more powerful and more secure than earlier versions of its  
3 own products and its competitors' products. Sales of Intel's processors and chipsets  
4 account for over 80 percent of the Company's total annual revenue. Intel has benefited  
5 from the explosive growth in data and the accompanying rise in cloud storage, holding a  
6 99 percent market share in servers that drive the cloud.

7 3. In June 2017, a team of researchers at Google's Project Zero – a unit that  
8 alerts technology companies to cyber security threats – privately informed Intel of two  
9 major vulnerabilities in Intel's processors, known as "Spectre" and "Meltdown." Spectre  
10 and Meltdown affect nearly every processor Intel has released since 1995. Both exposed  
11 data stored on nearly every modern electronic device with Intel processors to theft by  
12 hackers. Google provided Intel with proof, including code and test results, of actual attacks  
13 on an Intel processor that exposed "secure" information. Additional researchers  
14 independently corroborated the flaws and alerted Intel. Under established protocol,  
15 Google's Project Zero affords companies like Intel 90 days to either disclose or remediate  
16 the threat. Only in "extreme circumstances" will Google Project Zero extend the 90-day  
17 deadline.

18 4. Here, Spectre and Meltdown exploit fundamental design defects in Intel's  
19 processors. In other words, they are not manufacturing or physical defects or software  
20 bugs. Given that the defects exist in the fundamental architecture of Intel's processors, all  
21 software platforms are vulnerable regardless of the operating system. Consequently, a huge  
22 variety of electronic devices, personal computers, laptops, notebooks, desktops,  
23 smartphones, and servers are exposed. The defect is particularly problematic for "cloud"  
24 platforms, where huge numbers of networked computers routinely share and transfer data  
25 among thousands or millions of users.

26 5. Throughout the Class Period, Intel and its executives concealed Spectre and  
27 Meltdown while repeatedly claiming that its processors were more secure and faster than  
28 those of its prior versions and its competitors' products. The Company represented that its

1 latest generation of processors provided “rock-solid security” and a “critical layer of  
2 protection” from hackers, while boosting performance by 30, 40 and even 60% over  
3 previous generations. Rather than disclose the fundamental threat to its products,  
4 Defendants promoted the supposedly “unprecedented power and responsiveness,”  
5 “stronger protection,” and “built-in security” that made “password logins, browsing, and  
6 online payments safe and simple.” Indeed, Defendants falsely claimed Intel’s processors  
7 offered “strong security without compromising performance,” were “designed to secure  
8 the platform” and “optimized for data protection.” Defendants further represented that  
9 Intel’s processors “had the ability to protect against identity breaches” because their  
10 “hardware-based security technologies provide a critical foundation for secure IT” that  
11 “address the numerous, increasing, and evolving security threats across physical and virtual  
12 infrastructures.”

13 6. After being warned about Spectre and Meltdown, Defendants took  
14 undisclosed steps to attempt to mitigate the problems, privately working with industry  
15 players and select customers to develop and test software fixes or “patches” to address the  
16 problems. Unable to remediate the threats from Spectre and Meltdown within the 90-day  
17 window afforded by Google Project Zero, Intel sought and received a special extension of  
18 the confidential period to January 2018.

19 7. During this window, Chief Executive Officer Brian Krzanich unloaded 80%  
20 of his personal Intel holdings for more than \$40 million in November 2017. He sold every  
21 exercisable option and the maximum number of shares he could sell under the Company’s  
22 bylaws. As one analyst put it, “In all the years I’ve been at this and of all the companies  
23 I’ve covered, I can’t recall another massive sale of this scale.”

24 8. The truth started to emerge on January 2, 2018, when *The Register* reported  
25 that researchers had identified Meltdown. On this news, Intel’s stock plunged, wiping out  
26 billions of dollars in market capitalization.

27 9. On January 3, 2018, Defendants ultimately admitted to Spectre and  
28 Meltdown and that they were informed about the security flaws *more than 6 months ago*

1 in June 2017. Intel's stock price fell another 2%, erasing additional billions of dollars in  
2 market capitalization.

3 10. The market also learned that the defects can only be partially fixed, and at  
4 substantial cost to performance. The only effective long-term fix for Spectre is redesigning  
5 the processors. As one researcher put it, the threat from Spectre is "going to live with us  
6 for decades." Meltdown requires "kernel page table isolation" or a stronger wall around  
7 the computer kernel. But this workaround reduces performance between 5 and 30 percent.

8 11. On January 8, 2018, Krzanich acknowledged that fixes for Spectre and  
9 Meltdown would slow the performance of processors and that the problem may be more  
10 pervasive than Defendants originally represented. The next day Microsoft released data  
11 showing that the patches may "significantly" slow down the performance of certain servers  
12 and some personal computers ("PCs"). On this news, Intel's stock price declined another  
13 2.5%, a market capitalization loss of \$5.2 billion.

14 12. On January 10, 2018, *Forbes* reported that independent tests showed a  
15 "significant impact" on heavy processor workloads. Additional media sources similarly  
16 reported that Intel's data center customers were exploring using microprocessors from  
17 Intel's rivals to build new infrastructure. Intel's stock price fell another 2.6% on January  
18 10, a market capitalization loss of \$5.2 billion.

19 13. In the aftermath, Intel continued to struggle with Meltdown and Spectre and  
20 admits that "high risk" threats remain. In late January 2018, Intel warned PC and Mac  
21 users against installing the Company's patches because they could cause spontaneous  
22 reboots and other unpredictable system behavior. The patches, according to a prominent  
23 software engineer, were "COMPLETE AND UTTER GARBAGE." A former Intel leader  
24 in security services explained that there are 135 or more malware applications meant to  
25 exploit Spectre, Meltdown and issues with the patches. Intel, in May 2018, likewise  
26 confirmed reports of eight additional threats from the next generation of Spectre, each of  
27 which requires its own patches. Patches for four "high-risk" threats are unavailable until  
28 at least August 2018.

14. By this action, Lead Plaintiff seeks redress for losses it and other Intel investors suffered after purchasing common stock during the Class Period at artificially inflated prices.

## II. JURISDICTION AND VENUE

15. This Court has jurisdiction over the subject matter of this action under Section 27 of the Exchange Act, 15 U.S.C. § 78aa. In addition, because this is a civil action arising under the laws of the United States, this Court has jurisdiction under 28 U.S.C. §§ 1331 and 1337.

16. Venue is proper in this District under 28 U.S.C. § 1391(b) and Section 27 of the Exchange Act, 15 U.S.C. § 78aa. Intel is headquartered and conducts business in this District, and many of the acts and transactions that constitute the violations of law alleged in this Complaint, including the dissemination to the public of untrue statements of material facts, occurred in this District.

## III. PARTIES

### A. Plaintiff

17. On May 28, 2018, the Court appointed Louisiana Sheriffs as Lead Plaintiff under 15 U.S.C. § 78u-4(a)(3)(B). Louisiana Sheriffs is a multi-employer, defined benefit, governmental retirement plan providing retirement, disability and death benefits to approximately 25,000 active and retired employees of the sheriffs' offices in all 64 Louisiana parishes. As of June 30, 2016, Lead Plaintiff managed roughly \$3 billion in assets. As set forth in the attached certification, Louisiana Sheriffs purchased shares of Intel stock during the Class Period and suffered damages as a result of Defendants' violations of the federal securities laws.

### B. Defendants

18. Defendant Intel is a multinational technology company. Incorporated in Delaware, the Company maintains its corporate headquarters at 2200 Mission College Boulevard, Santa Clara, California 95054-1549, and its Internet website address is www.intel.com. Intel stock trades on NASDAQ under ticker symbol "INTC." As of

1 September 30, 2017, Intel had 4.68 billion shares of stock outstanding. Throughout the  
2 Class Period, Intel disseminated SEC filings, press releases, investor presentations, product  
3 descriptions, and other reports containing material misrepresentations and omissions about  
4 the security and performance of its processors.

5 19. Defendant Brian M. Krzanich (“Krzanich”) was CEO of Intel and a member  
6 of the board of directors until he was compelled to resign on June 21, 2018. During the  
7 Class Period, Krzanich made materially false statements and omissions about the security  
8 and performance of Intel’s microprocessors in the Company’s public filings, at investor  
9 presentations, and during conference calls. Krzanich also was present when the other  
10 Defendants made statements or omissions on these subjects without correcting them.  
11 Krzanich executed certifications relating to Intel’s false and misleading reports on Form  
12 10-Q for the third quarter of fiscal year 2017. Krzanich directly participated in the  
13 management and day-to-day operations of the Company and had actual knowledge of  
14 confidential proprietary information concerning the Company and its business, operations,  
15 and products. Krzanich also shared primary responsibility for ensuring that the Company’s  
16 SEC filings and other public statements or releases were complete, accurate, and did not  
17 omit material information necessary under the circumstances to make them not misleading.  
18 By signing and authorizing SEC filings and press releases that directed investors to the  
19 Company’s website for more information about Intel and its products, Krzanich  
20 represented that he had reviewed, approved of, and authorized the statements made on the  
21 website. Because of this position of control and authority, his ability to exercise power and  
22 influence over Intel’s conduct and his access to material inside information about Intel  
23 during the Class Period, Krzanich, at the time of the wrongs alleged herein, was a  
24 controlling person within the meaning of Section 20(a) of the Exchange Act. On June 21,  
25 2018, Krzanich resigned as Intel’s CEO and a member of the board of directors.

26 20. Defendant Robert H. Swan (“Swan”) was appointed Intel’s Executive Vice  
27 President, Chief Financial Officer (“CFO”) on October 10, 2016. Swan served in this  
28 capacity throughout the Class Period. As CFO during the Class Period, Swan oversaw

1 Intel's global finance organization, including finance, accounting and reporting, tax,  
2 treasury, internal audit, and investor relations; Information Technology; and the company's  
3 Corporate Strategy Office. During the Class Period, Swan made materially false statements  
4 and omissions about the security and performance of Intel's microprocessors in the  
5 Company's public filings, at investor presentations, and during conference calls. Swan  
6 also was present when the other Defendants made statements or omissions on these subjects  
7 that he knew to be false and misleading, yet took no steps to correct those statements. Swan  
8 executed certifications relating to Intel's false and misleading reports on Form 10-Q for the  
9 third quarter of fiscal year 2017. Swan directly participated in the management and day-  
10 to-day operations of the Company and had actual knowledge of confidential proprietary  
11 information concerning the Company and its business, operations, and products. Swan  
12 also shared primary responsibility for ensuring that the Company's SEC filings and other  
13 public statements or releases were complete, accurate, and did not omit material  
14 information necessary under the circumstances to make them not misleading. Swan  
15 possessed the power and authority to control, and approved of, the contents of the  
16 Company's press releases and investor and media presentations at all relevant times. By  
17 signing and authorizing SEC filings and press releases that directed investors to the  
18 Company's website for more information about Intel and its products, Swan represented  
19 that he had reviewed, approved, and authorized the statements made on the Company's  
20 website. Because of this position of control and authority, his ability to exercise power and  
21 influence over Intel's conduct and his access to material inside information about Intel  
22 during the Class Period, Swan, at the time of the wrongs alleged herein, was a controlling  
23 person within the meaning of Section 20(a) of the Exchange Act. On June 21, 2018, upon  
24 the resignation of Krzanich, Swan was named Intel's interim CEO.

25 21. Defendant Navin Shenoy ("Shenoy") is, and was at all relevant times, Intel's  
26 Executive Vice President and General Manager of the Data Center Group, Intel's business  
27 segment responsible for the Company's data-centric businesses, including server,  
28 network, and storage-related product lines. In this role, Shenoy oversees the strategy and

1 product development of Intel's data center platforms, a business that spans servers,  
2 networks, and storage across all customer segments. Approximately 90% of the Data  
3 Center Group's revenue is derived from platforms and related products impacted by the  
4 Meltdown and Spectre security flaws. At all relevant times, Shenoy had extensive  
5 operational and technical knowledge and experience, including with respect to Intel's  
6 processors. Shenoy began his career at Intel in 1995 and progressed through a series of  
7 leadership roles at Intel, including serving as the Company's Senior Vice President and  
8 General Manager of the Client Computing Group. During the Class Period, Shenoy  
9 provided information about the performance and security of the Data Center Group's  
10 processors that was incorporated into the Company's investor presentations and website  
11 statements, and reviewed and approved those statements. Shenoy was actively involved in  
12 the product launch and marketing of Intel's Xeon Scalable processors, and spoke about the  
13 performance and security features of Intel processors. After the Class Period, Shenoy  
14 spoke about the Company's efforts to address the security exploits, including the  
15 Company's firmware updates for its processors and testing results and data showing  
16 performance degradation to Intel's processors attributable to patches. During the Class  
17 Period, Shenoy made materially false statements and omissions about the security and  
18 performance of Intel's microprocessors in the Company's public filings, at investor  
19 presentations, and during conference calls. Shenoy also was present when the other  
20 Defendants made statements or omissions on these subjects that he knew to be false and  
21 misleading, yet took no steps to correct those statements. Shenoy directly participated in  
22 the management and day-to-day operations of the Company and had actual knowledge of  
23 confidential proprietary information concerning the Company and its business, operations,  
24 and products. Shenoy also shared primary responsibility for ensuring that the Company's  
25 SEC filings and other public statements or releases were complete, accurate, and did not  
26 omit material information necessary under the circumstances to make them not misleading.  
27 Shenoy possessed the power and authority to control, and approved of, the contents of the  
28 Company's website, press releases and investor and media presentations at all relevant

1 times. Because of this position of control and authority, his ability to exercise power and  
2 influence over Intel's conduct and his access to material inside information about Intel  
3 during the Class Period, Shenoy, at the time of the wrongs alleged herein, was a controlling  
4 person within the meaning of Section 20(a) of the Exchange Act.

5 22. Defendants Krzanich, Swan, and Shenoy are collectively referred to as the  
6 "Individual Defendants."

#### 7 **IV. SUMMARY OF THE FRAUD**

##### 8 **A. Intel, Its Products And Operating Groups**

9 23. Intel provides semiconductor chips and platforms for the worldwide digital  
10 economy. The Company designs, manufactures and sells a broad range of semiconductor  
11 products that include microprocessors, chipsets, motherboards, flash memory, and wired  
12 and wireless connectivity products. These components are integral to the functioning of  
13 computers, servers, smartphones, tablets, and networking and communications products.  
14 Intel also sells software primarily focused on security and technology integration. Intel  
15 competes against other chipmakers such as Advanced Micro Devices, Inc. ("AMD") and  
16 ARM Holdings ("ARM"), but the Company maintains a dominant position in the processor  
17 and server processor markets, producing about 90 percent of the world's processors for  
18 desktop and laptop computers and 99 percent of the server processors in the data centers  
19 that support the internet.

20 24. The Company's clients are the biggest companies in the technology industry,  
21 including Amazon, Apple, Dell, Facebook, Google, HP Inc., IBM, and Microsoft. The  
22 ultimate end users of Intel's processors include retail computer users, operating system  
23 vendors, cloud-service providers, and device manufacturers. The technology industry's  
24 dependence on Intel and the architectural design of its processors greatly increases the  
25  
26  
27  
28

1 exposure not only to potential security breaches but also to “shock events” that disrupt  
2 entire systems.<sup>1</sup>

3 25. Intel typically offers its products as “platforms.” A platform consists of a  
4 microprocessor and chipset. A microprocessor is a computer processor on a microchip and  
5 is the main component of all computers and is often referred to as the “brain” of a computer.  
6 The key functional block of a microprocessor is the Central Processing Unit, or CPU.<sup>2</sup> A  
7 microprocessor functions as a calculator that can quickly execute operations (add, subtract,  
8 multiply, divide, etc.) at billions of times per second. It processes data and controls other  
9 devices in the system. The microprocessor is a critical component impacting a computer’s  
10 performance and processing speed.

11 26. A chipset is the computer’s “nervous system.” It sends the data between the  
12 microprocessor and inputs, display, and storage devices such as keyboard, mouse, and  
13 monitor. The chipset performs essential logic functions and controls the access between  
14 the CPU and main memory.

15 27. The Company is the largest global supplier of the x86 series of  
16 microprocessors, which is the type of processor found in computers and laptops. Intel’s  
17 brand of x86 processors include the Core, Xeon, Atom, Celeron and Pentium processor  
18 families—some of the Company’s best-selling and most well-known processors.

19 28. On September 25, 2017, Intel launched its 8th generation Core “Coffee  
20 Lake” desktop processor. Familiar graphic designs for Intel’s processors appear below:  
21  
22  
23  
24  
25

---

26 <sup>1</sup> Max Chafkin and Ian King, *Intel Has a Big Problem. It Needs to Act Like It*, Bloomberg  
27 Businessweek (Jan. 18, 2018).

28 <sup>2</sup> Although technically distinct components, the terms processors, chips, CPUs often are  
used interchangeably.



29. Intel sells its processor platforms to a variety of customer segments, including:

a. Original Equipment Manufacturers (“OEMs”) that make (i) computer systems, (ii) cellular handsets and handheld computing devices, or (iii) networking communications equipment;

b. Original Design Manufacturers (“ODMs”) that provide design and manufacturing services to branded and unbranded private-label resellers;

1 c. Personal Computer and Network Communications Product Users (which  
2 include individuals, businesses, and service providers) who buy PC component and board-  
3 level products and networking & communication products through distributors, resellers,  
4 retail, and OEM channels;

5 d. Manufacturers and service providers, such as industrial and communication  
6 equipment manufacturers and cloud service providers who buy Intel's products through  
7 distributor, reseller, retail, and OEM channels; and

8 e. Government departments and agencies.

9 30. Intel manages its business through various operating groups, including:

10 a. Client Computing Group ("CCG"), which includes platforms designed for  
11 notebooks and desktops (including 2-in-1, thin-and-light, high-end desktop, and all-in-one  
12 PCs). It also includes wired and wireless connectivity products and mobile communication  
13 components. The CCG generates 54% of Intel's total revenue. Among the CCG platforms  
14 are the Intel® Core™ X-series and the 8th Gen Intel® Core™ processor families.

15 b. Data Center Group ("DCG"), which includes platforms and related products  
16 designed for enterprise, cloud and communication infrastructure market segments, and  
17 server, network, and storage platforms. The DCG generates 30% of Intel's total revenue.  
18 Among the DCG's platforms are the Intel® Xeon® Scalable processors.

19 c. Internet of Things Group ("IOTG"), which includes high-performance  
20 Internet of Things platforms for retail, automotive, and industrial market segments, as well  
21 as a broad range of other embedded applications. The IOTG generates 5% of Intel's total  
22 revenue.

23 31. As shown in the charts below, Intel's processor platforms have traditionally  
24 been the core offerings of the CCG, DCG and IOTG business segments and the Company  
25 as a whole. In particular, processor platforms have historically accounted for upwards of  
26 90% of these business segments' total revenues and over 80% of the Company's as a whole.  
27  
28

Years Ended (In Millions)	December 30, 2017		December 31, 2016		December 26, 2015	
<b>Client Computing Group</b>	Net Revenue	% of Sales	Net Revenue	% of Sales	Net Revenue	% of Sales
Platform	\$31,226	92%	\$30,751	93%	\$30,680	95%
Adjacent <sup>3</sup>	\$2,777	8%	\$2,157	7%	\$1,539	5%
<b>Data Center Group</b>	Net Revenue	% of Sales	Net Revenue	% of Sales	Net Revenue	% of Sales
Platform	\$17,439	91%	\$15,895	92%	\$14,856	93%
Adjacent	\$1,625	9%	\$1,341	8%	\$1,125	7%
<b>Internet of Things Group</b>	Net Revenue	% of Sales	Net Revenue	% of Sales	Net Revenue	% of Sales
Platform	\$2,645	83%	\$2,290	87%	\$1,976	86%
Adjacent	\$524	17%	\$348	13%	\$322	14%
<b>Total Net Revenue from Platform Products</b>					<b>% of Sales</b>	
<b>December 30, 2017</b>			\$53,310		82%	
<b>December 31, 2016</b>			\$48,936		82%	
<b>December 26, 2015</b>			\$47,512		86%	

Source: Intel's 2017 Annual Report at 75.

## **B. Intel's Quest To Develop Faster, More Powerful Processors**

32. Intel's success depends on continuously improving the power, speed, and performance of its processors. This requires constant improvements to the underlying

<sup>3</sup> The term "Adjacent" refers to non-platform products, such as modem, ethernet and silicon photonics.

1 technology. Intel's forecasted rate of progress is known as "Moore's Law."<sup>4</sup> Named after  
2 Intel's co-founder, Gordon Moore, Moore's Law predicts that "the number of transistors  
3 incorporated into a chip will approximately double every 24 months." Put differently,  
4 Moore observed that the number of transistors per chip doubled approximately every two  
5 years.

6 33. David House, a colleague of Moore's at Intel, later factored increased  
7 performance of transistors to conclude that performance of circuits would double every 18  
8 months.<sup>5</sup> This means that, every two years, the size of chips should decrease and their  
9 speed and performance more than double.

10 34. Decades ago, CPUs had "in order" designs; instructions were executed in the  
11 order they were received, with no attempt to reorder them or execute the instructions more  
12 efficiently. One of the major problems with "in order" execution was that computers would  
13 often stall where multiple instructions were given in parallel, stopping the CPU until the  
14 issue was resolved.<sup>6</sup>

15 35. With the release of its Pentium processors in 1995, Intel introduced a new  
16 "out of order" technology known as "speculative execution," which provides a platform  
17 for dramatic performance improvement over previous Intel processors and its competitors.  
18 Speculative execution improves a chip's efficiency by enabling the computer to predict the  
19 instructions most likely to be needed in the near future, align the instructions for optimal  
20 execution, as opposed to executing them in the order they came in, and then "speculatively"  
21 execute those instructions.<sup>7</sup> But as described below, the technique also introduced security  
22 flaws.

---

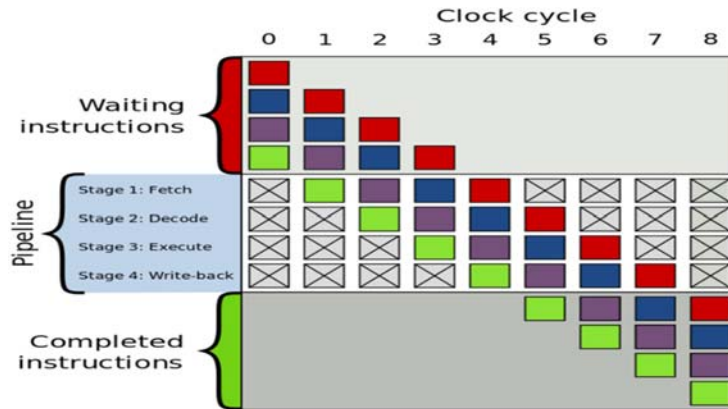
25 <sup>4</sup> Michael (Siyang) Li, *Keeping Up With Moore's Law*, Dartmouth Undergraduate J. of Sci.  
26 (May 29, 2013).

27 <sup>5</sup> *Id.*

28 <sup>6</sup> Joel Hruska, *What is Speculative Execution*, Extreme Tech (Jan. 10, 2018).

<sup>7</sup> *Id.*

36. Modern CPUs are all “pipelined,” which means they are capable of executing multiple instructions in parallel, as shown in the diagram below.<sup>8</sup>



37. In the diagram above, the green block represents an if-then-else branch. Using speculative execution, the CPU predicts which branch is more likely to be taken, fetches the next set of instructions associated with that branch, and begins speculatively executing them before it knows which of the two code branches it will be using. In the diagram above, these speculative instructions are represented as the purple box. If the branch predictor guessed correctly, then the next set of instructions the CPU needed are lined up and ready to go, with no pipeline stall or execution delay.<sup>9</sup>

38. Without branch prediction and speculative execution, the CPU does not know which branch it will take until the first instruction in the pipeline (the green box) finishes executing and moves to Stage 4. Instead of moving straight from one set of instructions to the next, the CPU has to wait for the appropriate instructions to arrive. This slows performance because it is time the CPU could otherwise be performing useful work.<sup>10</sup>

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

39. Speculative execution is now a key feature in modern processors, including the vast majority of processors produced by Intel. By continuously leveraging and refining this capability, Intel has been able to bring processors with the highest clock speeds and efficiency on the market over the past twenty years.

**C. Intel Assures Customers That Its Processors Provide Security**

40. In addition to improved performance, Intel customers have increasingly demanded security at the hardware level. The explosion in data and rapidly expanding dependence on computing devices to store and process that data, together with highly publicized data breaches, has created the need for processor manufactures to produce more secure chips for businesses and consumers to prevent exposure to malicious code, viruses, cyber espionage, malware, and data theft.

41. Intel, itself, has admitted that the growth in the hosting and scaling of data centers into cloud infrastructures has created entirely new security challenges and risks for businesses and consumers, stating, “[w]hile cloud technologies bring automation and agility to data center operations, they also challenge many of the underlying traditional security tools and physical control once enjoyed by IT. New security tools are needed to address growing security challenges, including assuring data confidentiality in the cloud and virtualized data centers—especially for mission-critical or sensitive data or workloads.”

42. To meet the rising demand for increased security, Intel consistently marketed that its processors offered “critical layers of protection” and were “designed to protect sensitive information.” Intel claimed that without compromising performance, it continued to enhance its processors to run more securely by providing “more robust, vulnerability-resistant platforms.” In doing so, Intel continually promoted the “rock-solid” security advances Intel embedded in the hardware of its processors, including identity protection technology, data encryption instructions, and platform trust technology.

43. Intel assured customers that with these security features, users would have unprecedented power and performance, all while protecting from hackers such sensitive

1 data as passwords, encrypted communications and other confidential information.

2 **D. Intel's Processors Sacrificed Security For Performance**

3 44. In truth, Intel's drive for performance and increased reliance on speculative  
4 execution compromised its chips' security. Although Intel's speculative execution  
5 increases efficiency, the process can introduce security flaws because it runs counter to the  
6 notion of process isolation. At its core, process isolation prohibits interprocess memory  
7 access. By restricting untrusted processes on a machine to a unique space, other areas of  
8 the machine containing sensitive information are protected. Process isolation protects data  
9 by preventing other processes or applications from observing or interfering with data in  
10 other restricted areas. Speculative execution undermines process isolation because it  
11 moves sensitive data from a computer's main memory to its less secure "cache" memory,  
12 where it can be processed more efficiently. This increases speed, but also leaves data more  
13 exposed because data in the "cache" memory is more vulnerable to unauthorized access  
14 than when it is stored in the main memory.

15 **E. Google Engineers Discover Flaws In Intel's Processors**

16 45. In or about July 2014, Google announced the formation of Project Zero, a  
17 full-time team of security analysts dedicated to finding vulnerabilities in Google software  
18 and any software or hardware employed by its users.

19 46. The Project Zero team uses a standard protocol for locating and reporting  
20 "zero day" vulnerabilities. Bugs discovered by Google's Project Zero team are filed in an  
21 external database and reported directly to the manufacturer on a confidential basis. Project  
22 Zero's findings become public once a patch has been released or when 90 days have passed  
23 without release of a patch. The day a company is notified of a vulnerability is known as  
24 "day zero" – and time runs for the next 90 days. The 90-day deadline gives software  
25 companies 90 days to fix a problem before informing the public, at which time the  
26 information is released so that users can take steps to protect themselves.

27 47. According to Google Project Zero, the 90-day deadline acknowledges an  
28 uncomfortable fact: the offensive security community invests considerably more into

vulnerability research than the defensive community. Therefore, when Google Project Zero finds a vulnerability in a high-profile target, it is often already known to advanced and stealthy actors. For these reasons, Google Project Zero has stated that it “adhere[s] to a 90-day disclosure deadline,” and even applies this approach for bugs Project Zero finds with respect to Google products. Google Project Zero only extends the deadline “based on extreme circumstances.”

48. In or about late April 2017, Jann Horn, an analyst from Google Project Zero analyzed Intel processor manuals for code Horn had created. Horn looked closely at how Intel’s microprocessors handle speculative execution. During his work, Horn discovered that if the microprocessor guessed wrong in anticipating instructions, the CPU nevertheless stored the data from those misguided forays in the microprocessors’ memory. Once there, the information is exposed to access by hackers. Horn also discovered that outsiders could “invert” instructions to force the processor to run new speculative executions, tricking the processor into retrieving and moving specific information into cache memory, where the hacker can access the information, including secret keys, passwords, or any other sensitive information stored on a computer.

49. Horn determined that this security flaw allowed unauthorized access into all areas of the computer’s memory, including the “kernel,” a crucial feature in ensuring that data in one program (or application) is not read by another. As detailed in Figure 1 below, the kernel connects the application software to the basic hardware of a computer, such as the CPU, the computer’s main memory, and the device itself.

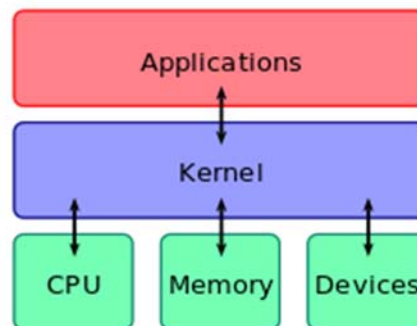


Figure 1

1           50. To maintain security, the kernel also acts as a barrier between the computer's  
2 main memory and other parts of a computer. The computer's main memory includes the  
3 computer's dynamic random-access memory ("DRAM"), as well as what is known as  
4 "kernel memory." Kernel memory is a protected area of memory used by the operating  
5 system and contains a computer's most confidential information, such as secret encryption  
6 keys, passwords and other sensitive information.

7           51. In consultation with other members of Google Project Zero, Horn developed  
8 test programs and successfully ran them against various Intel processors, as well as  
9 processors of Intel's competitors, AMD and ARM, verifying that this attack pattern on the  
10 processors' speculative execution could lead to the leaking of sensitive data, including from  
11 the kernel.

12           **F. Google Analysts Tell Intel About Spectre And Meltdown On June 1, 2017**  
13

14           52. On June 1, 2017, Horn provided a detailed report to Intel, AMD and ARM of  
15 "a CPU security issue that affects processors by Intel, AMD and (to some extent) ARM,"  
16 later known as "Spectre." The "bug report" described two "attack patterns" for exploiting  
17 speculative execution and "leaking" host memory: the branch-prediction variant and the  
18 array-bounds variant. The report provided test results, demonstrating that the programs led  
19 to the leaking of data on all three tested CPUs. The report explained that one way in which  
20 this security vulnerability could be abused on the Intel processors is by obtaining data in  
21 the computer's kernel. The report then set forth in detail the steps and codes for  
22 implementing such attacks on the computer's kernel, as well as test results demonstrating  
23 the "dump[ing] of kernel memory."

24           53. The report noted that Google Project Zero had not yet reported the bug to  
25 affected third parties, including Google, but concluded, "This bug is subject to a 90 day  
26 disclosure deadline. After 90 days elapse or a patch has been made broadly available, the  
27 bug report will become visible to the public."

28           54. Later in June 2017, Google Project Zero warned Intel about a second security

1 flaw exploiting speculative execution functions in Intel microprocessors, dubbed  
 2 “Meltdown.” While Meltdown presents different security risks than Spectre, like Spectre,  
 3 Meltdown is a security vulnerability that allows a hacker to “trick” a computer into moving  
 4 sensitive information into cache memory, where the hacker can access the information,  
 5 including secret keys, passwords and any other sensitive information stored on a  
 6 computer.<sup>11</sup>

7 55. Meltdown allows a hacker to move the highly sensitive data stored in kernel  
 8 memory to the cache memory. The hacker can then use any program on the computer to  
 9 access information moved to the cache memory (if the sensitive data were still in kernel  
 10 memory, the hacker would not be able to access it). One of the researchers who discovered  
 11 Meltdown described it as “probably one of the worst CPU bugs ever found.”<sup>12</sup>

12 56. Spectre and Meltdown impact nearly every Intel processor produced since  
 13 1995—approximately 90 percent of all Intel platforms, including those within the Core,  
 14 Xeon, Atom, Celeron and Pentium processor families. A list of all Intel-based processors  
 15 and platforms that Spectre and Meltdown affects is set forth below.<sup>13</sup>

16 **Core**

- 17 • Intel® Core™ i3 processor (45nm and 32nm)
- 18 • Intel® Core™ i5 processor (45nm and 32nm)
- 19 • Intel® Core™ i7 processor (45nm and 32nm)
- 20 • Intel® Core™ M processor family (45nm and 32nm)
- 21 • 2nd generation Intel® Core™ processors
- 22 • 3rd generation Intel® Core™ processors
- 23 • 4th generation Intel® Core™ processors
- 24 • 5th generation Intel® Core™ processors
- 25 • 6th generation Intel® Core™ processors
- 26 • 7th generation Intel® Core™ processors
- 27 • 8th generation Intel® Core™ processors
- 28 • Intel® Core™ X-series processor family for Intel® X99 platforms

25 <sup>11</sup> Samuel Gibbs, *Spectre and Meltdown processor security flaws – explained*, The  
 26 Guardian (Jan. 4, 2018).

27 <sup>12</sup> *Id.*

28 <sup>13</sup> <https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html>.

- Intel® Core™ X-series processor family for Intel® X299 platforms
- Xeon**
  - Intel® Xeon® processor 3400 series
  - Intel® Xeon® processor 3600 series
  - Intel® Xeon® processor 5500 series
  - Intel® Xeon® processor 5600 series
  - Intel® Xeon® processor 6500 series
  - Intel® Xeon® processor 7500 series
  - Intel® Xeon® processor E3 family
  - Intel® Xeon® processor E3 v2 family
  - Intel® Xeon® processor E3 v3 family
  - Intel® Xeon® processor E3 v4 family
  - Intel® Xeon® processor E3 v5 family
  - Intel® Xeon® processor E3 v6 family
  - Intel® Xeon® processor E5 family
  - Intel® Xeon® processor E5 v2 family
  - Intel® Xeon® processor E5 v3 family
  - Intel® Xeon® processor E5 v4 family
  - Intel® Xeon® processor E7 family
  - Intel® Xeon® processor E7 v2 family
  - Intel® Xeon® processor E7 v3 family
  - Intel® Xeon® processor E7 v4 family
  - Intel® Xeon® processor Scalable family
  - Intel® Xeon Phi™ processor 3200, 5200, 7200 series
- Atom**
  - Intel® Atom™ processor C series
  - Intel® Atom™ processor E series
  - Intel® Atom™ processor A series
  - Intel® Atom™ processor x3 series
  - Intel® Atom™ processor Z series
- Celeron**
  - Intel® Celeron® processor J series
  - Intel® Celeron® processor N series
- Pentium**
  - Intel® Pentium® processor J series
  - Intel® Pentium® processor N series

57. In or about September 2017, separate and apart from Google Project Zero, a group of five researchers – Paul Kocher, a well-known security researcher; Daniel Genkin of University of Pennsylvania and University of Maryland; Mike Hamburg of Rambus;

1 Moritz Lipp of Graz University of Technology; and Yuval Yarom of the University of  
2 Adelaide and Data61 – informed Intel they had discovered two variants of the Spectre bug.

3 58. Further, on December 4, 2017, a group of researchers at the Graz University  
4 of Technology – Moritz Lipp, Michael Schwarz, and Daniel Gruss – reported to Intel their  
5 discovery of the Meltdown flaw. In or about the same time in December 2017, Werner  
6 Haas and Thomas Prescher, security researchers at Cyberus Technology, also  
7 independently reported their discovery of the Meltdown vulnerability to Intel.

8 **G. Intel’s Obstacles To Fixing Or Mitigating The Security Defects**

9 59. The only way Intel can completely eliminate the Meltdown and Spectre flaws  
10 is to entirely redesign its chips. Replacing the chip with an existing chip would not resolve  
11 the issue because no available chip is free from the defect.<sup>14</sup>

12 60. Spectre cannot be mitigated with a patch because it is a problem with the  
13 fundamental way the processor is designed, and therefore requires the hardware (*i.e.*, the  
14 computer chip) to be replaced entirely.<sup>15</sup> According to Paul Kocher, the independent  
15 security researcher and consultant who co-discovered the Spectre flaws, Spectre is “going  
16 to live with us for decades.” He explained further that “This will be a festering problem  
17 over hardware life cycles. It’s not going to change tomorrow or the day after. . . It’s going  
18 to take a while.”

19 61. Kocher has explained that software vendors like Microsoft could input  
20 “speculation barriers” or fixes for the Spectre vulnerabilities in the source code for any  
21 conditional branch path that might lead to something going wrong. But if those barriers  
22 are placed in every conceivable spot within the source code that might be vulnerable to the  
23 flaws, it will destroy performance. And if they are not applied, attackers will still be able  
24 to exploit the Spectre flaws. As a result, vendors must carefully pick and choose where  
25

26 <sup>14</sup> Chris O’Brien, *CERT: Only Way To Fix Meltdown and Spectre Vulnerabilities Is To*  
27 *Replace CPU*, Venture Beat (Jan. 4, 2018).

28 <sup>15</sup> Cade Metz and Nicole Perlroth, *Researchers Discover Two Major Flaws in the World’s*  
*Computers*, N.Y. Times (Jan. 3, 2018).

they apply the fixes. Besides operating systems, Kocher said it is much harder to apply Spectre fixes to other types of modern software, such as databases and web servers, because those programs are used to receive data from untrusted sources. Hardware vendors, on the other hand, have applied microcode updates that modify the way the branch predictor works in the processor, but Kocher said those modifications have led to stability problems for the chips. Kocher called these fixes “a fairly unsatisfactory solution,” because the microcode updates are only available to the operating system and not applications on the affected system. They also lead to performance hits.<sup>16</sup>

62. The Meltdown flaw can be mitigated, however, by installing a “patch” of software code on a computer’s operating system. Although a security patch purportedly resolves the Meltdown flaw, as explained below, a patch significantly impacts and slows down computer performance.<sup>17</sup> One such fix, known as the Kernel Page Table Isolation, causes the computer program to slow down by up to 30 percent.<sup>18</sup>

63. Meltdown poses a particular problem for cloud computing services run by companies like Amazon, Google, and Microsoft. Given that Intel processors are used in more than 90 percent of the computer servers that support the internet and private business networks and operations, the ramifications were staggering. According to Andres Freund, an independent software developer who tested the software patch for the Linux operating system, that patch could impact performance of affected machines by 20 to 30 percent.<sup>19</sup>

#### **H. Intel Confirms Google Project Zero’s Findings**

64. As Intel later admitted in a letter to Congress and in the Company’s 2017

---

<sup>16</sup> Rob Wright, *Paul Kocher Weighs In On Spectre Flaws, Vulnerability Disclosure*, SearchSecurity (Apr. 28, 2018).

<sup>17</sup> Tom Warren, *Intel’s Processors Have a Security Bug and the Fix Could Slow Down PCs*, The Verge (Jan. 3, 2018).

<sup>18</sup> Rob Thubron, *Massive Security Flaw Found in Intel CPUs, Patch Could Hit Performance By Up to 30%*, Techspot (Jan. 3, 2018).

<sup>19</sup> Cade Metz and Nicole Perlroth, *Researchers Discover Two Major Flaws in the World’s Computers*, N.Y. Times (Jan. 3, 2018).

1 Annual Report, Google Project Zero researchers informed the Company of the Spectre and  
2 Meltdown vulnerabilities in June 2017. In response, the Company conducted a “detailed  
3 analysis” of the vulnerabilities in June and July 2017 that confirmed their existence.

4 65. Pursuant to Google Project Zero’s 90-day disclosure policy, the security  
5 vulnerabilities were supposed to be publicly disclosed in early September 2017. However,  
6 according to Google Project Zero’s issue tracker, an unusual “deadline grace” was granted  
7 to Intel on August 7, 2017, to extend Google’s 90-day disclosure deadline.

8 66. Without disclosure, Intel worked *for months* with a limited group of industry  
9 collaborators attempting to develop mitigations, test them, and prepare releases. Among  
10 those with whom Intel shared information on a confidential basis were Google, Amazon,  
11 Apple, and Microsoft. Before it disclosed to these companies the existence of the flaws  
12 and shared any other information about them, Intel required each to sign a non-disclosure  
13 agreement that strictly controlled use of the information.

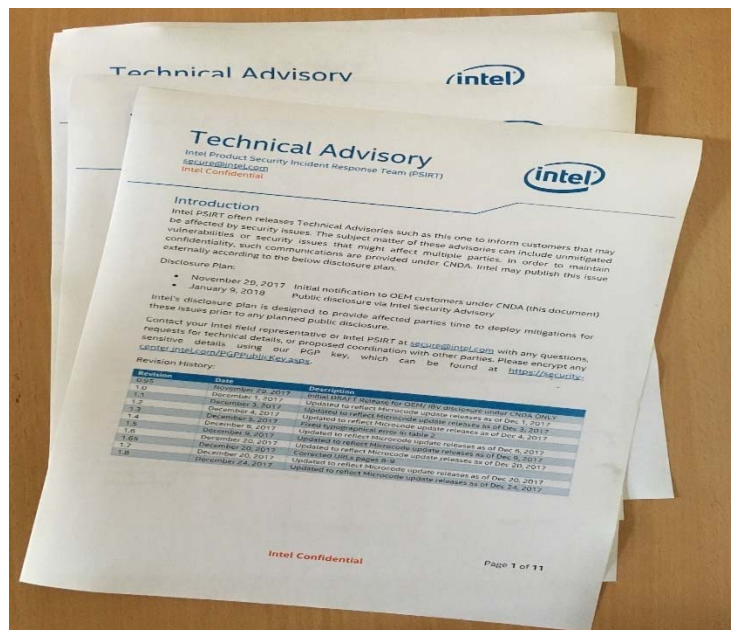
14 67. Government agencies around the world rely on computers, servers and  
15 networks powered by Intel processors. These agencies collectively face hundreds of  
16 millions of attempted hacks each day. To protect against the risk of these cybersecurity  
17 threats, the U.S. Government has established the United States Computer Emergency  
18 Readiness Team (“US-CERT”), which receives reports and addresses computer security  
19 incidents that affect the U.S. Government. US-CERT disclosure guidelines provide  
20 guidance for reporting such “incidents,” which are defined as an occurrence that actually  
21 or imminently jeopardizes the integrity and confidentiality of sensitive federal information.

22 68. Spectre and Meltdown fall squarely within this definition because they  
23 exposed to hackers sensitive information stored on government computers, servers and  
24 networks running on Intel processors. Nevertheless, Intel never warned or shared  
25 information with US-CERT, the National Security Agency (“NSA”), Homeland Security,  
26 any other government agency, or any other trusted third party in the vulnerability  
27 coordination and disclosure process such as the CERT Coordination Center (“CERT/CC”).  
28 An NSA spokesperson later confirmed that the agency first learned of the threat when news

1 broke publicly on January 3, 2018, adding, “we would have liked to have known.”

2 69. In a January 11, 2018 article published by *The Verge*, Will Dormann, a senior  
3 vulnerability analyst at CERT/CC confirmed that it was not notified when vulnerability  
4 was discovered. Dormann stated, “I would have liked to have known.” “If we’d known  
5 about it earlier, we would have been able to produce a more accurate document, and people  
6 would have been more educated right off the bat, as opposed to the current state, where  
7 we’ve been testing patches and updating the document for the past week.”<sup>20</sup>

8 70. While Intel failed to warn NSA, Homeland Security, US-CERT or CERT/CC  
9 about Spectre or Meltdown, the Company informed selected clients in or about November  
10 2017. The clients included Lenovo and Alibaba, two companies in which the Chinese  
11 government maintains large ownership stakes. On January 24, 2018, French technology  
12 publication LeMagIT, reported that it had obtained a copy of an 11-page confidential  
13 “Technology Advisory” memo sent to Intel’s OEM partners on November 29, 2017,  
14 notifying them for the first time of one of Spectre’s vulnerabilities under a confidential  
15 non-disclosure agreement.



28 <sup>20</sup> Russell Brandon, *Keeping Spectre Secret*, *The Verge* (Jan. 11, 2018).

1           71. The advisory, later updated on December 20, 2017, contains a “revision  
2 history” setting forth a schedule for the planned microcode updates for the Spectre  
3 vulnerability. According to the advisory, the first round of Spectre microcode updates,  
4 including those for several Broadwell and Haswell products, was made available to third  
5 parties on December 24, 2017. The advisory also includes a list of planned microcode  
6 updates scheduled for December 2017 to January 2018 for other Intel products, but did not  
7 offer specific dates for these updates.

8           72. Former Intel engineers describe the Company’s standard process or  
9 “playbook” for dealing with product threats. For example, a former Intel security engineer  
10 from 1999 to 2016, who had personal experience with previous PSIRT cases, provided the  
11 following description of the standard process the Company follows when it learns of threats  
12 like Spectre and Meltdown.

13           73. Intel has a standing, permanent team of people, known as the Product  
14 Security Incident Response Team (“PSIRT”), that is responsible for responding to threats  
15 or suspected vulnerabilities in Intel products. PSIRT also handles all communication and  
16 coordination with other affected entities, including OEMs and other customers for Intel  
17 products. PSIRT has several permanently assigned project managers, who bring in subject-  
18 matter experts from various affected departments to deal with specific threats. It is these  
19 subject matter experts who develop and test potential mitigations. In deciding which  
20 mitigation to select, the Company decides whether to take a performance hit across all  
21 products and users, or take a higher performance hit on only those products most vulnerable  
22 to the problem. The ultimate decision is made by people far up in the Company, including  
23 the “owner” or head of the impacted business unit. According to the “playbook” the  
24 Company follows in dealing with threats like Spectre and Meltdown, PSIRT managers  
25 immediately elevate the issue to the vice-president of the affected area, informing the VP  
26 that PSIRT has been engaged. For serious issues, the issues get elevated further to the  
27 senior VP level within a day or two. It then becomes the SVP’s responsibility to tell the  
28 CEO. Given the serious and widespread threat that Spectre and Meltdown posed to almost

1 all of Intel's microprocessors, the former security engineer had no doubt that the CEO  
2 would have been informed of the problems. The PSIRT also is responsible for developing  
3 a "disclosure plan" for informing OEMs, customers, and others about the problem and  
4 proposed mitigations. In addition to approving the mitigations to be deployed, the affected  
5 business owners also must approve the disclosure plan. Given that Spectre and Meltdown  
6 crossed so many product lines at Intel, this engineer expects that the CEO and CFO would  
7 have reviewed and approved the disclosure plan for Spectre and Meltdown.

8 74. A former Intel Lead Post-Silicon Validation Engineer in the Company's  
9 Hillsboro, Oregon office, who during their 18 years at the Company worked on servers that  
10 incorporated the Xeon processor before leaving the Company in January 2017, explained  
11 that Spectre and Meltdown affected so many products that it would have impacted all  
12 manner of Intel design teams and required a large and varied team to work on the  
13 mitigations.

14 75. A former Intel Senior Product Manager and Engineer of Manufacturing  
15 provided further detail based on his/her personal experience during their 10+ years at  
16 Intel's Columbia, South Carolina facility between 2007 and 2018. When Intel learns of  
17 bugs or security threats, it forms a team of people to investigate and respond. Members of  
18 the team are required to sign additional non-disclosure agreements regarding the specific  
19 issue they are working on. They also must sign an agreement "that bars them from trading  
20 stock they might have in Intel for some number of months after the information is made  
21 public." In developing and testing potential mitigations, performance slowdown  
22 "absolutely" would have been one of the things tested with any potential mitigations. CPU  
23 slowdown would have been tested on various platforms over various chips. With threats  
24 as large as Spectre and Meltdown, several tiered options would have been developed and  
25 tested. As Intel engineers tested potential mitigations, they would have logged the data and  
26 test results and presented their findings and recommendations to the senior executives in  
27 the business units directly impacted by Spectre and Meltdown. At these "forums," which  
28 the Company referred to as "war rooms," participants would discuss potential mitigations

1 and their impacts on performance. Because the Data Center Group was one of those units  
 2 directly impacted, Defendant Shenoy, as head of the Data Center Group, would have  
 3 participated in those discussions and would have made the “final call” on which mitigations  
 4 to deploy. Shenoy and other senior business leaders in turn would provide Krzanich, Swan  
 5 and other corporate executives with weekly or bi-weekly reports.

6 **I. Defendants Continued To Promote Security**  
 7 **And Performance, While Concealing Spectre And Meltdown**

8 76. Intel promoted the security and performance of its processors to investors in  
 9 multiple contexts, including marketing materials, press releases, quarterly SEC filings,  
 10 blog entries, investor presentations, and conferences.

11 77. In numerous SEC filings and press releases during the Class Period,  
 12 Defendants directed investors to visit Intel’s website for “information about Intel.” In the  
 13 Company’s 2016 Annual Report, which was referred to and incorporated in Intel’s SEC  
 14 filings during the Class Period, Defendants directed investors to visit the Company’s  
 15 website for “[n]ews and information about Intel® products and technologies.” Intel  
 16 continued to promote the security and performance of its next generation processors on its  
 17 website throughout the Class Period without disclosing Spectre and Meltdown.

18 78. When Intel launched its 8th generation Core “Coffee Lake” desktop  
 19 processor family (September 25, 2017, with October 5 availability), Intel’s website  
 20 repeatedly promoted these processors’ security, claiming that they were “Easy to Use, Hard  
 21 to Break Into” and offered “hardened security” and “hardware-enhanced security.” The  
 22 Company also stated that the processors’ “[b]uilt-in security adds a critical layer of  
 23 protection to make password logins, browsing, and online payments *safe and simple*” and  
 24 that the processors had “rock-solid security” features. The webpage also claimed that the  
 25 Core processors have “[h]ardware-level technologies that strengthen the protection of  
 26 enabled security software,” and that this “[h]ardware-based security helps you experience  
 27 online and offline activities with peace of mind.” Intel’s website further represented that  
 28 “Consumers benefit from protected internet and email content, plus fast, responsive disk

encryption.” At the same time, the website also promoted these processors’ speed and performance, claiming they delivered “amazing performance” and “Unprecedented Power and Responsiveness.” Intel broadcast the following statements and similar statements concerning its Core family processors throughout the Class Period:



### Get Unprecedented Power and Responsiveness

Now everyday computer tasks can happen faster. Edit photos and videos seamlessly. Move between programs and windows quickly. Multi-task easily. Better still, all that performance comes with up to 10 hours of battery life<sup>1,5</sup>, so you can take your computer wherever you go without worrying about cords and plug points.

### Easy to Use, Hard to Break Into

Built-in security<sup>6</sup> adds a critical layer of protection to make password logins, browsing, and online payments safe<sup>6</sup> and simple. You can log on with a look, your voice, or your fingerprint for rock-solid security<sup>6</sup> that's fast and hassle free. Store passwords, personal information, and auto-fill information with one master password. Plus touch screen, voice commands, and stylus options offer natural and intuitive interactions.

79. Intel’s website made similar representations regarding the security and performance of its Xeon family processors during the Class Period, telling the public that the processors’ had “[g]roundbreaking architecture” that provides improved security and compression performance in cloud, networking, big data, and storage applications,” that

the processors “[c]reate a Silicon-Based Trusted Infrastructure” that “optimize interconnectivity with a focus on speed without compromising data security,” and that users could “[d]eploy hardware-enhanced security to protect data and system operations without compromising performance.” Intel broadcast the following statements and similar statements concerning its Xeon family processors throughout the Class Period:



## ENSURE TRUST, RESILIENCE, AND CONTROL

Intel® technology enables Trusted Infrastructure through a suite of platform security technologies built into Intel® silicon. Hardware-based security technologies provide a critical foundation for secure IT. They address the numerous, increasing, and evolving security threats across physical and virtual infrastructures.

80. In addition, Intel’s website promoted the security and performance of its Atom processors during the Class Period, claiming that they provided “enhanced performance,” and that they had “improved security features” and that “[b]uilt-in security features help you avoid malware, protect your identity, and keep your data safe.”

81. Intel’s website made similar claims regarding its Pentium® and Celeron® processors during the Class Period, claiming that the processors had “[s]ecurity you can trust,” while concurrently providing “30% more processor performance.” In particular, Intel made extensive representations regarding the purported “protection capabilities” of these processors:

Protection capabilities in the Intel® Pentium® and Celeron® processors are built from the ground up to give you a device you can trust. Every time you start it up, secure boot with Intel® Platform Trust Technology helps keep your device safe, blocking dangerous programs, so only trusted software is launched. You get peace of mind with a more secure operating environment. Execute Disable Bit defends against ever-elusive malware, reducing your exposure to viruses and malicious code attacks. It works behind the scenes,

1 so you don't have to think about it, and it shuts down malicious code before  
2 it can take root.

3 It's easy to secure all your data with Advanced Encryption Standard (AES)  
4 and Secure Hash Algorithm (SHA) new instructions built into the processor.  
5 You get strong security without compromising performance or impacting  
6 your experience.

7 ...the peace of mind that it will give you the performance, experiences, and  
8 security you want.

9 82. Intel also posted videos promoting the security of its products, claiming that  
10 Intel processors' "hardware-based protection" had "the ability to protect against identity  
11 breaches with multi-factor authentication in the hardware protecting the factors, the policy  
12 and the credentials."

13 83. These statements were false, misleading and omitted material facts. In truth,  
14 Intel's Core, Xeon, Atom, Pentium® and Celeron® processors all contained major security  
15 flaws that exposed sensitive data to hackers. Specifically, Defendants concealed from  
16 investors that the Spectre and Meltdown vulnerabilities exposed users' data to theft.  
17 Defendants further misled investors by concealing that the only permanent solution to  
18 address Spectre and Meltdown was a fundamental redesign of Intel's processors, and that  
19 the patches being developed to mitigate the vulnerabilities until a permanent fix could be  
20 developed were ineffective and significantly impaired the processors' performance,  
21 especially for heavy workload users like cloud clients. After the Class Period, Defendants  
22 admitted that the patches degraded performance and belatedly disclosed that the patches  
23 may make published performance benchmarks "inapplicable" to users' devices or systems.

24 84. Intel publicly promoted the security and performance of its processors to  
25 investors in multiple other contexts. For example, on July 11, 2017, after being warned  
26 about the serious threats that Spectre and Meltdown attacks posed, the Company hosted a  
27 conference to unveil the "Purley" version (now known as Xeon Scalable) of its Xeon server  
28 processor family.

85. In connection with the conference, Defendants issued a press release stating,





90. Intel similarly promoted the performance of the Company's 8th Gen Intel® Core™ and Intel® Xeon® Scalable processors in its Form 10-Q filed with the SEC for the fiscal quarter ended September 30, 2017. In a section titled "Management Discussion and Analysis of Financial Conditions and Results of Operations," the 10-Q stated the 8th Generation Intel® Core Processors code named "Coffee Lake" delivered "significant performance improvements to our client platforms."

91. On Intel's earnings call that same day, Defendant Krzanich stated, "We've made great progress in both our data-centric and PC-centric businesses over the last few months . . . . We're especially excited about the launch of our latest Eighth Generation Core processor, codenamed Coffee Lake. The Coffee Lake family includes our first 6-core desktop CPU. And it's our best gaming processor to date, *with up to 50% better performance than the competition on top-game titles.*" (Emphasis added.)

92. Analysts responded well to Defendants' positive statements. J.P. Morgan, for example, reported on October 27, 2017, that "Given the performance benefits of Xeon Scalable over the prior Broadwell architecture, we anticipate a strong refresh cycle continuing through 2018." Analysts from Northland Capital Markets noted that "Intel is driving far greater value through its growing portfolio of refreshed server chips (launched Purley)." Likewise, analysts at Roth Capital Partners predicted that "the steady upgrade cycle around newer Xeon Scalable products [would] represent a multi-quarter tailwind for the company."

93. On October 27, 2017, Defendants continued to market its "high performance" products on the Company's website with an article titled, "Unlocking Data Insights With The Powerful Intel Xeon Scalable Processor." In the article, Defendants praised "[t]he recently launched Intel® Xeon® Scalable Processor family," claiming that it "provides powerful performance for the widest variety of workloads, including a 1.73X average performance boost vs. the previous generation across key industry-standard workloads." Defendants also highlighted the Xeon® Scalable processors' security qualities, stating that it is "[a]rchitected with increased memory and IO bandwidth, *as well*

1 *as advanced security features.*” (Emphasis added.)

2 94. On November 6, 2017, Defendants again plugged the performance of its 8th  
3 Gen Intel Core processor, when they published an article titled, “Intel Editorial: New Intel  
4 Core Processor Combines High-Performance CPU With Custom Discrete Graphics From  
5 AMD to Enable Sleeker, Thinner Devices.” Defendants noted that the “new addition to  
6 the 8<sup>th</sup> **Gen Intel Core** processor family builds on our strong portfolio of mobile and  
7 graphics solutions.” Defendants further stated, “Now, we’re opening the door for thinner,  
8 lighter devices across notebooks, 2 in 1s and mini desktops, while delivering incredible  
9 performance and graphics for enthusiasts.”

10 95. Similarly, on November 6, 2017, Defendants published, “Intel® Xeon®  
11 Scalable Processors Deliver A Big Boost In Simulation Performance.” Intel stated that  
12 “[t]he Intel® Xeon® Gold 6148 processor – part of the new Intel® Xeon® Scalable  
13 processor family – boosts performance for ANSYS Fluent\* 18.1 by up to 41 percent versus  
14 a previous-generation processor; and, its provides up to 34 percent higher performance per  
15 core, which helps contain licensing costs.” The article continued, “A key focus of the  
16 optimization effort was to improve vectorization in the solver code to leverage the  
17 advanced vector processing capabilities of Intel® Xeon® processors.” Defendants also  
18 cited results of benchmark tests of Intel Xeon® Gold 6148 processor, stating it “can  
19 improve performance for ANSYS Fluent by up to 41 percent versus a previous-generation  
20 server based on the Intel® Xeon® processor E5-2697 v4, and by as much as 60 percent  
21 versus a comparable server based on earlier Intel® Xeon® processor E5-2698 v3.”

22 96. Analysts, still in the dark about Spectre and Meltdown, again took note of  
23 Intel’s marketing. For example, on November 9, 2017, analysts at CrispIdea Research  
24 identified the Company’s roll-out of Xeon® Scalable processors as a “key development”  
25 in the Company’s product performance, remarking that “Intel® Xeon® Scalable  
26 processors” were set to “deliver disruptive performance efficiency across a diverse range  
27 of cloud workloads.”  
28

97. Following Defendants' publication of the articles above, on November 14, 2017, Defendant Shenoy presented at the UBS Global Technology Conference, and again promoted the performance and security features of Xeon® Scalable processors. Specifically, Shenoy stated that the Company's "Xeon architecture [] has been in the market for over 20 years now. It's proven. It's very much battle tested. It has outstanding performance on a wide range of workloads *that are designed to optimize not only performance, but security and agility of various workloads in the data center.*" (Emphasis added.) Shenoy further stated on November 14, 2017, that "Xeon Scalable outperforms on throughputs, kind of benchmarks by 34%, by 18% on performance per watt benchmarks and by over 50% on performance per core."

98. Analysts accepted Defendants' statements concerning the "outperformance" of Intel's microprocessors. On November 16, 2017, analysts at Canaccord Genuity stated, "Overall, with the launch of CoffeeLake, very select 10nm CannonLake notebook products and the Purley server platform ramp, we anticipate stronger 2H/17 results for Intel overall."

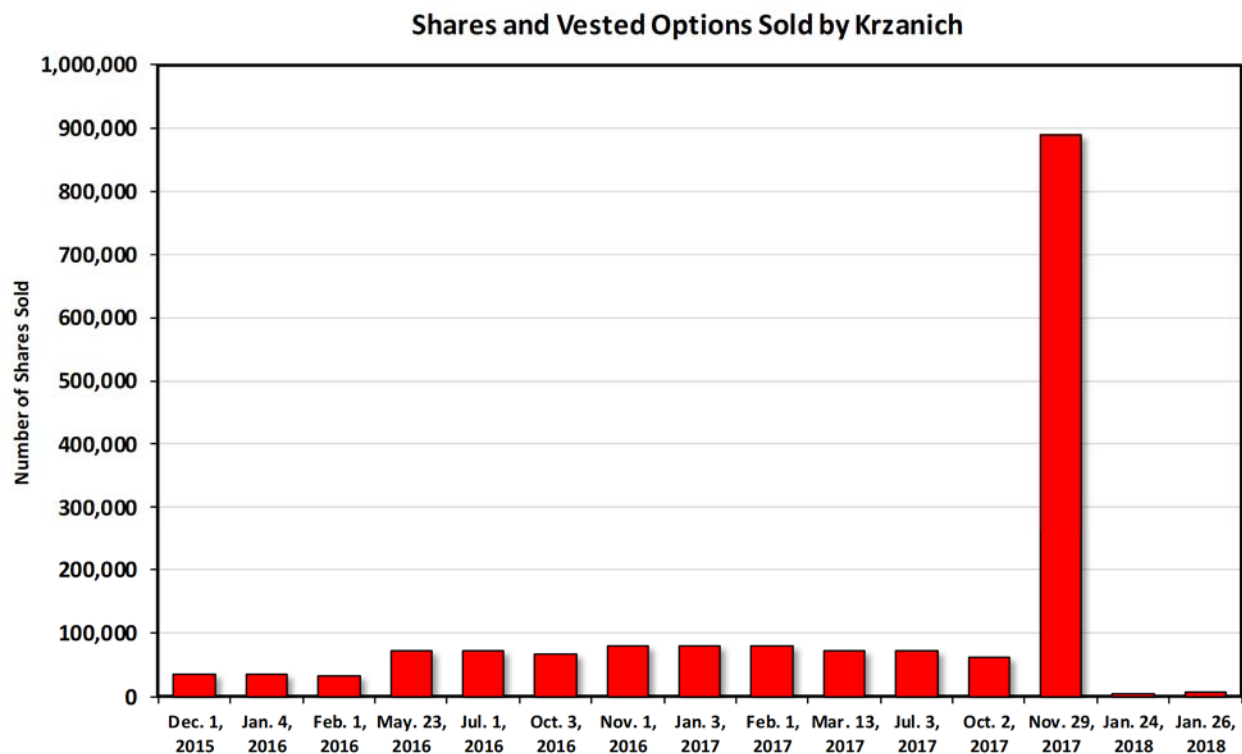
99. On November 28, 2017, Defendant Swan presented at the Credit Suisse Technology, Media and Telecom Conference. Swan emphasized the PC team's performance, stating, "they know how to execute in this market, and they've done it in a variety of different ways. First, annual product cadence and increased performance for our customers. That's been happening in the past. That's happening now. That will continue to happen in the future." Swan also addressed analysts' questions concerning the roll out of Intel® Xeon® Scalable processors, emphasizing that Intel® Xeon® Scalable processors were meeting Intel's cloud customers Chief Information *Officers'* "*increasing demand to be more efficient but to also deal with more cybersecurity threats.*" (Emphasis added.)

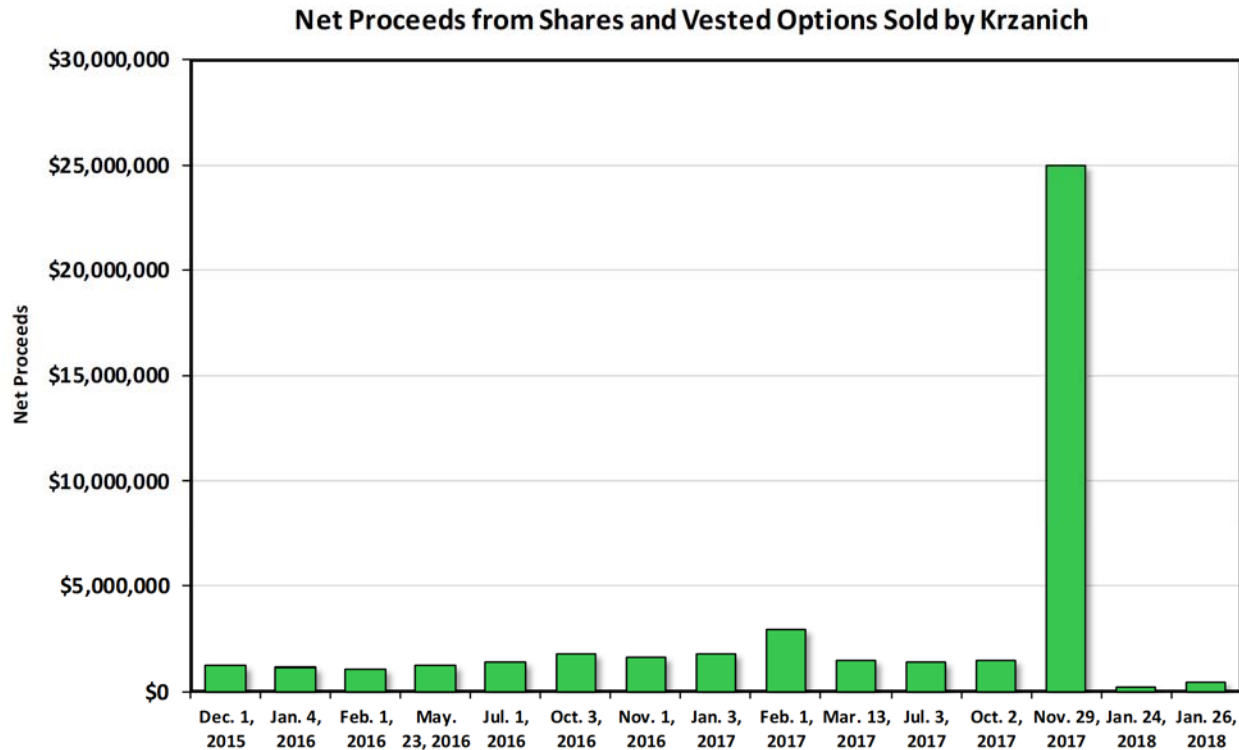
#### **J. Krzanich's Insider Trading**

100. On November 29, 2017 – the same day that Intel informed its OEM partners about Spectre – Krzanich sold 890,000 shares of Intel stock for nearly \$40 million, netting almost \$25 million in profits. Krzanich exercised and sold every exercisable option, even

though none were set to expire for at least 14 months, and sold every share he could while still maintaining the minimum shares the Company's bylaws required him to hold. All totalled, he sold 100% of the shares he was allowed to sell and 80% of his total holdings. These sales marked a complete deviation from Krzanich's previous pattern of incremental sales. According to SEC records, Krzanich had exercised options and sold shares at monthly or quarterly intervals in the previous two years. He never sold more than 80,000 shares in any of those sales. Thus, the number of shares Krzanich sold near the end of the Class Period was more than 10 times greater than any other sale in the previous 2 years, and his profits 8½ times larger than any other sale and 16 ½ times larger than the average sale during those 2 years. The timing of the sale allowed him to benefit greatly from the huge run-up in Intel's stock price, while avoiding any decline that the looming disclosure of Spectre and Meltdown would cause.

101. The following charts graphically depict Krzanich's sales:





102. Krzanich sold his shares under a Rule 10b5-1 plan that he modified 30 days before he unloaded his shares. But under Rule 10b5-1, a plan may be established or modified only when the corporate insider has no material nonpublic information (“MNPI”) about the Company or its securities.

103. Defendant Krzanich’s stock sales violated Intel’s Code of Conduct.<sup>21</sup> The Code restricts securities trading by “[a]ny employee who is aware of material, non-public information regarding Intel.”

104. According to a former Intel lead software and firmware engineer in the Company’s Hillsboro, Oregon office, who held many positions at Intel between 2005 and 2017, every Intel employee is required to take Intel’s online Code of Conduct class each year. The purpose of the class is to educate employees on recurring ethical issues and to reinforce that anything that seems like a violation is grounds for termination. The class

<sup>21</sup> <https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/2018-intel-code-of-conduct.pdf>.

1 begins with a 3-minute video of Krzanich explaining how important it is for Intel  
2 employees to act ethically and understand the Company's Code of Conduct. One of the  
3 specific topics covered during the online class is insider trading. Employees are instructed  
4 that "anything that looks like insider trading or might feel like insider trading can be  
5 considered insider trading, and it can get you fired."

6 **K. The Truth Emerges Through A Series Of Partial Disclosures**

7 105. Intel and market participants had initially planned to simultaneously disclose  
8 the existence of the vulnerabilities and deploy the mitigations on January 9, 2018. But on  
9 January 2, 2018, after the market closed, British technology website *The Register* released  
10 a story titled, "Kernel-memory-leaking Intel processor design flaw forces Linux, Windows  
11 redesign: Speed hits loom, other OSes need fixes."<sup>22</sup> In the article, *The Register* disclosed  
12 the vulnerability now called "Meltdown," reporting that it was "a fundamental design flaw"  
13 that impacted "modern Intel processors produced in the past decade." The article explained  
14 that the vulnerability allows programs "to access a [computer's] kernel memory." *The*  
15 *Register* reported that to fix the flaw, providers of major operating systems, such as Linux  
16 and Microsoft, are instituting software patches to isolate the kernel memory, but these  
17 updates may handicap the performance of Intel chips by up to 30%.

18 106. On January 3, 2018, the price of Intel stock fell 3% from \$46.85 per share on  
19 January 2, 2018, to \$45.26 per share, the worst day for the Company's stock in over a year,  
20 wiping out \$7.44 billion of market capitalization.

21 107. On January 3, 2018, after the market closed, Intel accelerated its own planned  
22 disclosure of the problems. In a press release, Intel admitted that it "ha[d] been made aware  
23 of new security research describing software analysis methods that, when used for  
24 malicious purposes, have the potential to improperly gather sensitive data from computing  
25 devices that are operating as designed." Intel, however, attempted to downplay the issue,  
26 claiming media reports about the flaws were "incorrect" and "inaccurate" and that the  
27

28 <sup>22</sup> [https://www.theregister.co.uk/2018/01/02/intel\\_cpu\\_design\\_flaw/](https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/).

1 Company's competitors' chips were similarly impacted. The Company noted that it had  
2 begun providing software and firmware updates to mitigate the exploits, but contrary to  
3 some media reports, "any performance impacts are workload-dependent, and, for the  
4 average computer user, should not be significant and will be mitigated over time."

5 108. In or about the same time, on January 3, 2018, after trading hours, Google  
6 Project Zero published its findings on the security variants it had discovered and  
7 communicated to Intel in June 2017. Google Project Zero revealed to the public that Intel  
8 and other manufacturers' processors suffered from another variant now called "Spectre."  
9 Google Project Zero's report described that like Meltdown, Spectre also breaks the  
10 isolation between different applications and allows hackers to trick programs into leaking  
11 a users' confidential information. However, unlike Meltdown, Spectre makes it possible  
12 for a program to access data in a separate program, without any need to call on the operating  
13 system or kernel memory. News outlets such as *Bloomberg* reported that this attribute  
14 makes Spectre more difficult to fix, as any fix would require more than simply isolating  
15 the kernel memory.

16 109. Immediately thereafter, on January 3, 2018, Defendant Krzanich appeared  
17 for an interview on CNBC. On the segment, Krzanich admitted that "we were made aware  
18 of this issue a while back from Google researchers" and had been working with all the  
19 Company's industry partners, including operating system vendors and OEMs, to patch and  
20 resolve the problem. Krzanich assured the public that "we believe we have the right fixes  
21 in place. We've been testing those fixes and making sure that we understand how to  
22 implement those."

23 110. Later that same evening, on January 3, 2018, Intel hosted a conference call  
24 to address Spectre and Meltdown. Stephen Smith, the Company's General Manager of  
25 Data Center Engineering, admitted that Intel engineers and industry partners had "been  
26 working for months with the participants in the industry to align the different pieces." That  
27 effort involved "multiple microprocessor vendors, operating system vendors and OEMs  
28 around the world" working to understand the issue and "to develop the system software

1 updates, to develop the firmware and to integrate and test those things.” For some of the  
2 flaws, Intel was required to change some firmware that resides with the processor.

3 111. Ronak Singhal, an Intel Fellow and Director of CPU Compute Architecture,  
4 explained further that mitigating the vulnerabilities would require software, firmware, and  
5 hardware improvements or fixes: “So the strategy here requires both updates on the  
6 software side as well as on the hardware side.” Although Singhal explained that Intel  
7 already had rolled out software patches to address the vulnerabilities, he implicitly admitted  
8 that those were not permanent solutions and that hardware fixes would be needed to address  
9 security and performance issues: “we will be pursuing hardware initiatives or hardware  
10 improvements for both performance and security going forward.” He described how the  
11 mitigations would require migration from firmware and software fixes to hardware:  
12 “Basically, as we have the ability to move this from the firmware and software domain into  
13 the hardware, we’re able to lessen the impact while providing security.”

14 112. The former Intel lead software and firmware engineer discussed above, who  
15 worked in the CPU division for a year early in his career at Intel, confirmed that the  
16 permanent fix would be in the CPU hardware because a microcode fix would degrade  
17 performance of the chip. The hardware change needed for a permanent fix could take  
18 anywhere from one to two years to develop depending on Intel’s design flow.

19 113. The price of Intel stock declined from \$45.26 per share on January 3, 2018,  
20 to \$44.43 per share on January 4, 2018, or approximately 2%, wiping out an additional  
21 \$3.8 billion of market capitalization.

22 114. On January 4, 2018, Intel issued a press release, announcing that the  
23 Company had developed and was rapidly issuing updates for all types of Intel-based  
24 computer systems — including personal computers and servers — that render those  
25 systems immune from both the Spectre and Meltdown exploits. Intel further represented  
26 that it “continues to believe that the performance impact of these updates is highly  
27 workload-dependent and, for the average computer user, should not be significant and will  
28 be mitigated over time.” However, that same day, the National Cybersecurity and

1 Communications Integration Center (“NCCIC”) expressed concerns about the efficacy of  
2 the patches in an alert it published on January 4, 2018, warning that the patches could  
3 diminish performance by up to 30% and represented only a partial solution: “Due to the  
4 fact that the vulnerability exists in CPU architecture rather than in software, patching may  
5 not fully address these vulnerabilities in all cases.”

6 115. On January 8, 2018, after trading hours, news outlets reported on Defendant  
7 Krzanich’s presentation at The International Consumer Electronics Show (“CES”) 2018  
8 given earlier that evening, reporting that Krzanich indicated that fixes for Spectre and  
9 Meltdown would cause a bigger slowdown and that the problem may be more pervasive  
10 than Defendants originally represented. At the conference, Krzanich provided an update  
11 on Intel’s efforts to release patches, stating, “for our processors and products, introduced  
12 in the past five years, Intel expects to issue updates for more than 90 percent within a week,  
13 and the remaining [updates will be available] by the end of January.” Krzanich admitted,  
14 however, that some users’ performance would be affected more than others, stating, “we  
15 believe the performance impact of these updates is highly workload dependent.” We expect  
16 some workloads may experience a larger impact than [sic] others, so we’ll continue working  
17 with the industry to minimize the impact on those workloads over time.”

18 116. The following day, on January 9, 2018, additional information came to light  
19 undermining Intel’s statements of the severity of the problem. In particular, before trading  
20 hours, *DigiTimes* reported that Intel held several meetings with computer vendors at the  
21 end of 2017 to discuss resolutions for its processors’ security flaw issue, but failed to come  
22 to a conclusion. Citing vendors and market watchers, *DigiTimes* reported that industry  
23 watchers believe the impact on PC demand will not emerge until around mid-February  
24 2018, and that the extent of harm to PC demand still needs to be monitored and the impact  
25 could undermine vendors’ PC shipments during the first half of 2018.

26 117. Later that same day, Microsoft provided new data about the performance  
27 impact of fixes to the security vulnerabilities. Specifically, Microsoft cautioned that  
28 computers underpinning corporate data centers and networks, used for certain tasks, may

1 show “more significant impact” and see a “significant” slow down on performance  
2 resulting from the fixes. Microsoft further announced that PCs running Windows 10 and  
3 sold since 2016 will face slowdowns of approximately 10 percent.

4 118. These partial disclosures caused Intel’s stock price to decline. On January 9,  
5 2018, shares of Intel fell \$1.12, or 2.5%, a loss of \$5.2 billion in market capitalization.

6 119. On January 9, 2018, after trading hours, news sources reported that United  
7 States Senators Jack Reed and John Kennedy had written a letter to the Justice Department  
8 and the SEC requesting they investigate Defendant Krzanich’s sale of stock and options.  
9 The Senators wrote:

10 Dear Chairman Clayton and Attorney General Sessions:

11 We write to request that the Securities and Exchange Commission and the  
12 Department of Justice investigate the alarming reports that Intel’s Chief  
13 Executive Officer sold more than \$20 million of his Intel securities on  
14 November 29, 2017. While news reports suggest that these securities were  
15 sold pursuant to an automatic trading plan, known as a Rule 10b5-1 plan, we  
16 are disturbed by additional reports that the instructions for these securities  
17 transactions were adopted on October 30, 2017, which is before the public  
18 was made aware of serious cybersecurity flaws in Intel’s chips but months  
19 after Google informed Intel in June of these security vulnerabilities.

20 These reports are troubling not only because of the risk to nearly all phones  
21 and computers, but also because these reports raise concerns of potential  
22 insider trading. We request that you conduct a thorough examination of  
23 whether any insider trading laws were violated. Furthermore, if you uncover  
24 such violations through your examination, we expect you to enforce our laws  
25 to the fullest extent possible.

26 120. On January 10, 2018, before trading hours, *Forbes* published an article titled,  
27 “Meltdown Fixes Will Slow Intel Computers – Here’s All The Proof You Need.” The  
28 article reported that results from independent tests carried out by security researcher  
Thomas Roth had showed that “[b]usinesses running large-scale, heavy workloads on their  
servers could see a significant impact.” In particular, Roth tested an updated Intel i7-6700  
processor running Ubuntu 16.04 with Linux Kernel 4.14.11 and found “severe issues with  
system calls (the requests made by programs to the kernel, the heart of the operating system

1 helping run all other software),” observing they “were four times slower after the patch.”  
2 *Forbes* quoted Roth as saying, “I believe the main impact will be on really large scale  
3 environments such as search engines, large web-sites and cloud-providers, where even a  
4 5% increase of the base workload requires additional hardware.”

5 121. Later, on January 10, 2018, many other news sources similarly reported that  
6 because of the security vulnerabilities, Intel’s data center customers, whose computers run  
7 cloud networks, were exploring using microprocessors from Intel’s rivals to build new  
8 infrastructure.

9 122. On this news, shares of Intel fell \$1.12, or 2.6% on January 10, 2018, erasing  
10 \$5.2 billion in market capitalization.

11 **L. Patches Are Ineffective**

12 123. On January 11, 2018, Defendant Shenoy admitted in a blog post that Intel  
13 had received reports from customers that the patches were causing problems. Shenoy  
14 nonetheless told customers they should continue applying the patches.

15 124. On January 22, 2018, however, only two weeks after reassuring investors and  
16 the public that the Company had developed software patches to mitigate the vulnerabilities  
17 that would have “negligible” performance impacts for most users, Intel suddenly warned  
18 PC and Mac users not to install the patches because they could cause major problems.  
19 Defendant Shenoy admitted that deploying the patches “may introduce higher than  
20 expected reboots and other unpredictable system behavior,” and apologized “for any  
21 disruption this change in guidance may cause.” Linus Torvalds, a prominent software  
22 engineer and principal developer of the Linux kernel that became the basis for operating  
23 systems such as Linux, Android, and Chrome OS, was unsparing in his criticism of Intel’s  
24 paltry attempt to mitigate the vulnerabilities, describing the patches as “COMPLETE AND  
25 UTTER GARBAGE” in a message posted to the Linux kernel mailing list and quoted in  
26 numerous articles.

27 125. A former Intel Senior Global Lead in Security Services in the Hillsboro,  
28 Oregon office from 2015 to 2017, who has followed developments with Spectre and

1 Meltdown in his/her security services role at his/her new company, confirmed that there  
2 was a problem with Intel's initial patch, which at one point incurred another security  
3 vulnerability. Based on this former employee's current work, he/she believes there are now  
4 135 or more malware items meant to exploit Spectre and Meltdown and security patches.  
5 While he/she did not work directly on the mitigation project, he/she knows that the  
6 vulnerability was all about the processor pre-fetching information. His/Her understanding  
7 is that the only way to permanently fix the vulnerabilities was either to cripple or entirely  
8 shut off that feature, which would cause a huge reduction in performance.

9 126. In early April 2018, Intel issued new "microcode revision guidance" that  
10 revealed the Company had stopped trying to develop microcode patches for many of the  
11 Company's processors. The guidance explained that microcode revisions had stopped for  
12 a number of chipsets because, "after a comprehensive investigation of the  
13 microarchitectures and microcode capabilities of these products, Intel has determined to  
14 not release microcode updates for these products for one or more reasons." One of the  
15 reasons given was "[m]icro-architectural characteristics that preclude a practical  
16 implementation of features mitigating [Spectre] Variant 2." In other words, the Company  
17 admitted it was unable to develop a practical solution to the Spectre vulnerabilities for those  
18 processors.

19 127. A month later, a German computer magazine reported that security  
20 researchers had identified eight additional Spectre flaws, which they dubbed Spectre-NG  
21 or Next Generation. Intel confirmed those reports on May 21, and further admitted to a  
22 new Meltdown-type flaw. Four of the Spectre-NG flaws are considered "medium risk" and  
23 four "high risk." Each of the eight additional vulnerabilities requires its own patches. Intel  
24 has confirmed that patches for the four "high-risk" vulnerabilities will not be available until  
25 at least August 2018.

26 128. Intel's patches not only failed to eliminate the threats from Spectre and  
27 Meltdown, they also have adversely impacted performance of the Company's processors.  
28 Intel has admitted that performance tests on the Company's latest generation of Core

processors saw performance declines of 2 to 14 percent. Intel has further admitted that users with heavy workloads should expect performance declines of 30% or more. These numbers are consistent with analyses that other industry participants have performed, including Red Hat, Inc., the world's leading provider of open source software solutions for cloud computing, enterprise management, virtualization, and data storage. The problem is particularly acute for users with large storage workloads, with tests reported to reveal performance declines of 20 to 60 percent.

129. Indeed, after the Class Period, Intel revised published statements on its website about the purported performance of its processors by adding a footnote to make clear that these results “were obtained prior to implementation of recent software patches and firmware updates intended to address exploits referred to as ‘Spectre’ and ‘Meltdown’” and that implementation of these patches “may make these results inapplicable to your device or system.”

## **V. DEFENDANTS’ FALSE AND MISLEADING STATEMENTS AND OMISSIONS**

130. Defendants made false and misleading statements and material omissions during the Class Period regarding the security and performance of Intel’s processors in violation of Sections 10(b) and 20(a) of the Exchange Act, and Rule 10b-5 promulgated thereunder. As further explained below, Defendants’ representations were false and misleading and omitted material facts, including that the processors were subject to major security vulnerabilities that allowed hackers to access users’ most sensitive personal information, and that fixing the flaws will significantly impair the processors’ performance.

### **A. Statements On Intel’s Website**

131. Throughout the Class Period, Defendants published numerous false or misleading statements on Intel’s website about the “enhanced” security features and increased performance of the Company’s processors. In numerous SEC filings and press releases throughout the Class Period, Defendants directed investors to visit Intel’s website for “information about Intel®.” In the Company’s 2016 Annual Report, which was referred

1 to and incorporated in Intel’s SEC filings during the Class Period, Defendants directed  
 2 investors to visit the Company’s website for “[n]ews and information about Intel®  
 3 products and technologies.”

4 132. Throughout the Class Period, Defendants published the following statement  
 5 about its Intel® Core™ processors on its Company website:

6 A new computer with a new 8th Generation Intel® Core™ processor helps you stay  
 7 ahead of the digital world. ***Get a big jump in performance*** compared to the previous  
 8 generation. Experience vivid gaming and content creation, immerse yourself in  
 leading-edge 4K UHD entertainment.

9 **Get Unprecedented Power and Responsiveness**

10 Now everyday computer tasks can happen faster. Edit photos and videos  
 11 seamlessly. Move between programs and windows quickly. ***Multitask easily.***  
***Better still, all that performance comes with up to 10 hours of battery life . . .***

12 **Easy to Use, Hard to Break Into**

13 ***Built-in security adds a critical layer of protection*** to make password logons,  
 14 browsing, and online payments ***safe and simple***. You can log on with a look, your  
 15 voice, or your fingerprint for ***rock-solid security*** that’s fast and hassle free. Store  
 16 passwords, personal information, and auto-fill information with one master  
 password. Plus touch screen, voice commands, and stylus options offer natural and  
 intuitive interactions.

17 133. These statements were false and misleading, and omitted material facts. In  
 18 truth, there are fundamental design flaws in Intel’s® Core™ processors that seriously  
 19 compromise the processors’ security and render them vulnerable to hacking and other  
 20 exploits. In particular, Defendants concealed from investors that the Spectre and Meltdown  
 21 vulnerabilities exposed users’ data to theft. Defendants further misled investors by  
 22 concealing that the only permanent solution to address Spectre and Meltdown was a  
 23 fundamental redesign of the Core™ processor, and that the patches developed to mitigate  
 24 the vulnerabilities until a permanent fix could be developed were ineffective and  
 25 significantly impaired the processors’ performance, especially for heavy workload users.  
 26 After the Class Period, Defendants admitted that the patches degraded performance and  
 27 belatedly disclosed that patches “may make these results inapplicable to your device or  
 28 system.” See ¶129.

134. Throughout the Class Period, Defendants published the following statement regarding its Intel® Core™ X-series processors on its Company website:

**Features At-a-Glance**

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI). A fast, secure AES engine for a variety of encryption apps, including whole disk encryption, file storage encryption, conditional access of HD content, *internet security*, and VOIP. *Consumers benefit from protected internet and email content, plus fast, responsive disk encryption.*

135. These statements were false and misleading, and omitted material facts. In truth, there are fundamental design flaws in Intel's® Core™ X-series processors that seriously compromise the processors' security and render them vulnerable to hacking and other exploits. Specifically, Defendants concealed from investors that the Spectre and Meltdown vulnerabilities exposed users' data to theft. Defendants further misled investors by concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign of the Core™ X-series processors, and that the patches developed to mitigate the vulnerabilities until a permanent fix could be developed were ineffective and significantly impaired the processors' performance, especially for heavy workload users.

136. Throughout the Class Period, Defendants published the following statements regarding its 8th Gen Intel® Core™ i7 processors on its Company website:

**Features and Performance**

**Get Unprecedented Power and Responsiveness**

Now everyday computer tasks can happen faster. Edit photos and videos seamlessly. Move between programs and windows quickly. Multitask easily. Better still, all that *performance comes with up to 10 hours of battery life*, so you can take your computer wherever you go without worrying about cords and plug points.

**Easy to Use, Hard to Break Into**

*Built-in security adds a critical layer of protection* to make password logons, browsing, and online payments safe and simple. You can log on with a look, your voice, or your fingerprint for *rock-solid security* that's fast and hassle free. Store passwords, personal information, and auto-fill information with one master password. Plus touch screen, voice commands, and stylus options offer natural and intuitive interactions.

**Intel® Online Connect**

With Intel® Online Connect, *security is built-in 7th Generation Intel® Core™ processors and above*, which adds a *layer of protection* to make browsing and online payments safe and simple.

Defendants made identical statements about Intel's® Core™ i3 and Intel's® Core™ i5 processors during the Class Period.

137. These statements were false and misleading, and omitted material facts. In truth, there are fundamental design flaws in Intel's® Core™ i3, i5, and i7 processors that seriously compromise the processors' security and render them vulnerable to hacking and other exploits. Specifically, Defendants concealed from investors that the Spectre and Meltdown vulnerabilities exposed users' data to theft. Defendants further misled investors by concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign of Intel's® Core™ i3, i5, and i7, and that the patches developed to mitigate the vulnerabilities until a permanent fix could be developed were ineffective and significantly impaired the processors' performance, especially for heavy workload users. After the Class Period, Defendants admitted that the patches degraded performance and belatedly disclosed that patches "may make these results inapplicable to your device or system." See ¶129.

138. Based on the timing, content, and Intel's practices, Defendants published the following statement regarding its 8th Generation Intel® Core™ processor family on its Company website during the Class Period:

**Prepare To Be Amazed With The 8th Generation Intel® Core™ Desktop Processor Family**

**DISCOVER THE BENEFITS**

1 - *Exceptional platform performance* with up to six cores for more processing power

...

3 - *Hardware-level technologies that strengthen the protection of enabled security software*

...

***Ultimate Protection Built Into the Silicon***

8th Generation Intel® Core™ processors integrate hardware-level technologies that strengthen the protection of your ***enabled security software***. ***Hardware-based security*** helps you experience online and offline activities with peace of mind, enabled by features that include:

- Intel® Software Guard Extensions (Intel® SGX) to help applications protect your system and your data
- Intel® BIOS Guard and Intel® Boot Guard to help protect your system during startup

139. These statements were false and misleading, and omitted material facts. In truth, there are fundamental design flaws in Intel's® Core™ processor family that seriously compromise the processors' security and render them vulnerable to hacking and other exploits. Specifically, Defendants concealed from investors that the Spectre and Meltdown vulnerabilities exposed users' data to theft. Defendants further misled investors by concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign of the Core™ processor family, and that the patches developed to mitigate the vulnerabilities until a permanent fix could be developed were ineffective and significantly impaired the processors' performance, especially for heavy workload users. After the Class Period, Defendants admitted that the patches degraded performance and belatedly disclosed that patches "may make these results inapplicable to your device or system." See ¶129.

140. Throughout the Class Period, Defendants published the following statement regarding its 7th Generation Intel® Core® vPro™ processor on its Company website:

Performance That Unleashes Productivity.

Security That's Hardware-Enhanced.

7th Generation Intel® Core® vPro™ processor

...

***Hardware-Enhanced Security***

***Built-in protection runs deeper than just software.***

***63% of data breaches start with misused or stolen credentials. Intel Authenticate Solution provides a robust multifactor verification solution that is protected in hardware, reducing exposure to software-level attacks***

...

***Multifactor verification.***

Customize your policy to protect against today's most common threat with multiple factors, including protected PIN, Bluetooth technology proximity, fingerprint, and location detection using Intel Active Management Technology (Intel AMT).

141. These statements were false and misleading, and omitted material facts. In truth, there are fundamental design flaws in 7th Generation Intel® Core® vPro™ processor that seriously compromise the processors' security and render them vulnerable to hacking and other exploits. Specifically, Defendants concealed from investors that the Spectre and Meltdown vulnerabilities exposed users' data to theft. Defendants further misled investors by concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign of the Core™ vPro processor, and that the patches developed to mitigate the vulnerabilities until a permanent fix could be developed were ineffective and significantly impaired the processors' performance, especially for heavy workload users. After the Class Period, Defendants admitted that the patches degraded performance and belatedly disclosed that patches "may make these results inapplicable to your device or system." See ¶129.

142. Throughout the Class Period, Defendants published the following statement regarding its Intel® vPro™ platform on its Company website:

Intel® vPro™ Platform - Increase Productivity and ***Data Security***

Explore how Intel® vPro™ platform business solutions increase productivity, improve manageability, and ***provide security*** for business transactions. Learn more about how this platform improves performance by creating faster multitasking ***with optimal data security***. This easily deployable business platform creates a stable environment that will keep your business up and running smoothly.

***Performance***

The latest Intel Core vPro processors.... Results in amazingly responsive systems that increase productivity for all workers. ...

***Security*** – Hardware-Enhanced Data Encryption ***Intel Data Guard technology***  
 Hardware-Enhanced Identity Protection ***Intel Authenticate Solution***

143. These statements were false and misleading, and omitted material facts. In truth, there are fundamental design flaws in Intel’s® vPro platform that seriously compromise the processors’ security and render them vulnerable to hacking and other exploits. Specifically, Defendants concealed from investors that the Spectre and Meltdown vulnerabilities exposed users’ data to theft. Defendants further misled investors by concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign of the vPro platform, and that the patches developed to mitigate the vulnerabilities until a permanent fix could be developed were ineffective and significantly impaired the processors’ performance, especially for heavy workload users. After the Class Period, Defendants admitted that the patches degraded performance and belatedly disclosed that patches “may make these results inapplicable to your device or system.” See ¶129.

144. Throughout the Class Period, Defendants published the following statement regarding its Intel® Xeon® Scalable processors on its Company website:

**Take a Major Leap Forward**

New Intel® Xeon® Scalable processors are workload-optimized to support hybrid cloud infrastructures and the most high-demand applications. You can drive actionable insight, ***count on hardware-based security***, and deploy dynamic service delivery.

**Advanced Features Are Designed into the Silicon**

Synergy among compute, network, and storage is built in. ***Intel® Xeon® Scalable processors optimize interconnectivity with a focus on speed without compromising data security.*** Here are just a few of the value-added features:

...

***Improve Security***

***Deploy hardware-enhanced security to protect data and system operations without compromising performance.***

145. These statements were false and misleading, and omitted material facts. In truth, there are fundamental design flaws in Intel’s® Xeon® Scalable processors that

seriously compromise the processors' security and render them vulnerable to hacking and other exploits. Specifically, Defendants concealed from investors that the Spectre and Meltdown vulnerabilities exposed users' data to theft. Defendants further misled investors by concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign of the Intel® Xeon® Scalable processors, and that the patches developed to mitigate the vulnerabilities until a permanent fix could be developed were ineffective and significantly impaired the processors' performance, especially for heavy workload users. After the Class Period, Defendants admitted that the patches degraded performance and belatedly disclosed that patches "may make these results inapplicable to your device or system." See ¶129.

146. Throughout the Class Period, Defendants published the following statement regarding its Intel® Xeon® Scalable processors on its Company website:

Create a Silicon-Based Trusted Infrastructure

The Intel® Xeon® Scalable platform delivers an essential, hardware-based root-of-trust environment. Protection extends up from the silicon, through the platform hardware and firmware, ensuring an effective IT security platform

Ensure Trust, Resilience, and Control

Intel® technology enables Trusted Infrastructure through a suite of platform security technologies built into Intel® silicon. ***Hardware-based security technologies provide a critical foundation for secure IT. They address the numerous, increasing, and evolving security threats across physical and virtual infrastructures.***

147. These statements were false and misleading, and omitted material facts. In truth, there are fundamental design flaws in Intel's® Xeon® Scalable processors that seriously compromise the processors' security and render them vulnerable to hacking and other exploits. Specifically, Defendants concealed from investors that the Spectre and Meltdown vulnerabilities exposed users' data to theft. Defendants further misled investors by concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign of the Intel® Xeon® Scalable processors, and that the patches

1 developed to mitigate the vulnerabilities until a permanent fix could be developed were  
 2 ineffective and significantly impaired the processors' performance, especially for heavy  
 3 workload users. After the Class Period, Defendants admitted that the patches degraded  
 4 performance and belatedly disclosed that patches "may make these results inapplicable to  
 5 your device or system." See ¶129.

6 148. Throughout the Class Period, Defendants published the following statement  
 7 regarding its Intel® Xeon® E3 processors on its Company website:

8 Intel® Xeon® E3 processors deliver *essential performance* and visuals to support  
 9 the needs of businesses worldwide, including: small business servers, powerful  
 10 mobile workstations, entry workstations, storage servers, cloud workstations, media  
 transcode and edge computing/IoT.

#### 11 **Professional Workstations**

12 Step up to the *essential performance* and visuals demanded professional CAD and  
 13 media workstation customers. Experience the difference of *professional-grade*  
 14 *compute performance* with enhanced memory capabilities, *hardware-enhanced*  
*security*, and reliability features and support for the latest Intel graphics.

#### 15 **Reliability for Small Business**

16 No matter what the size of your business, the value of your data is enormous. *Keep*  
 17 *it accessible and better protected*, with *hardware-enhanced performance*, at all  
 18 times, with an affordable Intel® Xeon® E3-1200 v6 processor-based small business  
 server.

19 149. These statements were false and misleading, and omitted material facts. In  
 20 truth, there are fundamental design flaws in the Intel® Xeon® E3 processors that seriously  
 21 compromise the processors' security and render them vulnerable to hacking and other  
 22 exploits. Specifically, Defendants concealed from investors that the Spectre and Meltdown  
 23 vulnerabilities exposed users' data to theft. Defendants further misled investors by  
 24 concealing that the only permanent solution to address Spectre and Meltdown was a  
 25 fundamental redesign of the Intel® Xeon® E3 processors, and that the patches developed  
 26 to mitigate the vulnerabilities until a permanent fix could be developed were ineffective  
 27 and significantly impaired the processors' performance, especially for heavy workload  
 28 users. After the Class Period, Defendants admitted that the patches degraded performance

1 and belatedly disclosed that patches “may make these results inapplicable to your device  
2 or system.” *See* ¶129.

3 150. Throughout the Class Period, Defendants published the following statement  
4 regarding its Intel® Xeon® processor E3 v3 family, the Intel® Xeon® processor E5 family,  
5 and the Intel® Xeon® processor E7 family on its Company website:

6 Data Protection with Hardware-Assisted Security

7 Ensuring Data Protection Through Innovation

8 The rapidly expanding dependence on computing devices creates the need for more  
9 secure software and hardware products for businesses and consumers to prevent  
10 exposure to malicious code, viruses, cyber espionage, malware, and data theft. This  
11 is also one of the drivers behind the rapid growth in cloud computing architectures  
12 for enterprises and consumers alike.

13 The hosting and scaling of data centers into cloud infrastructures creates new  
14 security challenges and risks for businesses and consumers. While cloud  
15 technologies promise to bring automation and agility to data center operations, they  
16 also challenge many of the underlying traditional security tools and physical control  
17 once enjoyed by IT. New tools are needed to address growing security challenges,  
18 such as establishing visibility to the state of the servers and assuring data  
19 confidentiality in the cloud and virtualized data centers—especially for mission-  
20 critical or sensitive data or workloads.

21 Intel continues to enhance systems so they run more securely. A key component of  
22 this approach is providing ***more robust, vulnerability-resistant platforms***. Security  
23 features are embedded in the hardware of Intel® processors, including three of  
24 Intel's newest server processors—the Intel® Xeon® processor E3 v3 family, the  
25 Intel® Xeon® processor E5 family, and the Intel® Xeon® processor E7 family, as  
26 well as the latest generation Intel® Core™ vPro™ processors.

27 151. These statements were false and misleading, and omitted material facts. In  
28 truth, there are fundamental design flaws in Intel® Xeon® processor E3 v3 family, the  
Intel® Xeon® processor E5 family, and the Intel® Xeon® processor E7 family that  
seriously compromise the processors’ security and render them vulnerable to hacking and  
other exploits. Specifically, Defendants concealed from investors that the Spectre and  
Meltdown vulnerabilities exposed users’ data to theft. Defendants further misled investors  
by concealing that the only permanent solution to address Spectre and Meltdown was a

fundamental redesign of the Intel® Xeon® processor E3 v3 family, the Intel® Xeon® processor E5 family, and the Intel® Xeon® processor E7 family, and that the patches developed to mitigate the vulnerabilities until a permanent fix could be developed were ineffective and significantly impaired the processors' performance, especially for heavy workload users.

152. Throughout the Class Period, Defendants published the following statement regarding its Intel® Pentium® and Celeron® processors on its Company website:

### **Intel® Pentium® and Celeron® Processors**

#### **DISCOVER THE BENEFITS**

- 1 - Enjoy more computing and greater graphics longer
- 2 - Uncompromised user experience at entry system price
- 3 - *Security you can trust*
- 4 - Choose from a wide range of mobile form factors

With up to **30% more processor performance** and 45% better graphics on Windows than the previous generation platform, the latest **Intel® Pentium® and Celeron® processors** give your platform the computing and visual power you've wanted.

#### ***Security You Can Trust***

**Protection capabilities** in the **Intel® Pentium® and Celeron® processors** are built from the ground up to give you a device you can trust. Every time you start it up, **secure boot** with Intel® Platform Trust Technology helps keep your **device safe, blocking dangerous programs**, so only trusted software is launched. You get peace of mind with a **more secure operating environment**. Execute Disable Bit defends against ever-elusive malware, reducing your exposure to viruses and malicious code attacks. It works behind the scenes, so you don't have to think about it, and it shuts down malicious code before it can take root.

It's **easy to secure all your data** with Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) new instructions built into the processor. You get **strong security without compromising performance or impacting your experience**.

153. These statements were false and misleading, and omitted material facts. In truth, there are fundamental design flaws in Intel® Pentium® and Celeron® processors that seriously compromise the processors' security and render them vulnerable to hacking and other exploits. Specifically, Defendants concealed from investors that the Spectre and

Meltdown vulnerabilities exposed users' data to theft. Defendants further misled investors by concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign of the Intel® Pentium® and Celeron® processors, and that the patches developed to mitigate the vulnerabilities until a permanent fix could be developed were ineffective and significantly impaired the processors' performance, especially for heavy workload users. After the Class Period, Defendants admitted that the patches degraded performance and belatedly disclosed that patches "may make these results inapplicable to your device or system." *See* ¶129.

### **B. October 26, 2017 3-Q 2017 Results**

154. On October 26, 2017, four days before Defendant Krzanich modified his 10b5-1 plan, Intel filed with the SEC its quarterly report for the third quarter of fiscal 2017 on Form 10-Q. In the section titled, "Management Discussions and Analysis of Financial Conditions and Results of Operations," Intel stated, "During the quarter, we launched our 8th Generation Intel® Core™ Processors, code named Coffee Lake, *which delivered significant performance improvement to our client platforms.*"

155. That same day, Defendants held a quarterly investor conference call during which Defendant Krzanich stated, "We're especially excited about the launch of our latest Eighth Generation Core processor, codenamed Coffee Lake. The Coffee Lake family includes our first 6-core desktop CPU. And it's our best gaming processor to date, *with up to 50% better performance than the competition on top-game titles.*"

156. Defendants' statements made in the Form 10-K and investor conference call on October 26, 2017, were false and misleading, and omitted material facts. In truth, there are fundamental design flaws in Intel's 8th Generation Intel® Core™ processors, code named Coffee Lake, that seriously compromise the processors' security and render them vulnerable to hacking and other exploits. Specifically, Defendants concealed from investors that the Spectre and Meltdown vulnerabilities exposed users' data to theft. Defendants further misled investors by concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign of the 8th Generation Intel®

Core™ Processors, and that the patches developed to mitigate the vulnerabilities until a permanent fix could be developed were ineffective and significantly impaired the processors' performance, especially for heavy workload users. After the Class Period, Defendants admitted that the patches degraded performance and belatedly disclosed that patches "may make these results inapplicable to your device or system." See ¶129.

**C. October 27, 2017 Intel Publication -  
Unlocking Data Insights With The  
Powerful Intel Xeon Scalable Processor**

157. On October 27, 2017, Intel published on the Company's website an article titled "Unlocking Data Insights With The Powerful Intel Xeon Scalable Processor," which focused on Intel's recent launch of the Intel® Xeon® Scalable processor. In the article, Defendants stated, "The recently launched Intel® Xeon® Scalable Processor family provides powerful performance for the widest variety of workloads, including *a 1.73X average performance boost* vs. the previous generation across key industry-standard workloads. Architected with increased memory and IO bandwidth, as well as *advanced security features*, Intel Xeon Scalable Processors are optimized to deliver 2.2X higher deep learning training and up to *2.4X higher inference performance* compared to the prior generation."

158. These statements were false and misleading, and omitted material facts. In truth, there are fundamental design flaws in the Intel® Xeon® Scalable processors that seriously compromise the processors' security and render them vulnerable to hacking and other exploits. Specifically, Defendants concealed from investors that the Spectre and Meltdown vulnerabilities exposed users' data to theft. Defendants further misled investors by concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign of the Intel® Xeon® Scalable processors, and that the patches developed to mitigate the vulnerabilities until a permanent fix could be developed were ineffective and significantly impaired the processors' performance, especially for heavy workload users. After the Class Period, Defendants admitted that the patches degraded performance. See ¶129.

**D. November 14, 2017 UBS Global Technology Conference**

159. On November 14, 2017, Defendant Shenoy presented at the UBS Global Technology Conference. During that conference, Defendant Shenoy offered a Company Investor Relations Presentation, where on slide 9, Defendants stated,

“Intel Xeon Scalable Processor  
Leadership vs. other x86 offerings 34% more performance, 53% more perf.  
Per core 18% more perf. Per watt.”

160. During the conference, Shenoy made further statements regarding the Xeon® Scalable platform, including:

This represents -- this product, the Xeon Scalable Skylake platform -- represents the biggest advancement that we’ve delivered in about a decade in terms of generation-on-generation performance gains. We delivered about a 1.65x improvement gen-on-gen. I mean, that's more than we would typically do in a gen-on-gen advancement.

And so I wanted to show you a couple of charts to demonstrate the performance leadership we believe we have. This Xeon architecture, of course, has been in the market for over 20 years now. It’s proven. It’s very much battle tested. ***It has outstanding performance on a wide range of workloads that are designed to optimize not only performance but security and agility of various workloads in the data center.***

The chart on the top shows the Xeon Scalable versus other x86 offerings in the marketplace. Using published benchmark data, we believe that Xeon Scalable outperforms on throughputs kind of benchmarks by 34%, by 18% on performance per watt benchmarks and by over 50% on performance per core, which is an important metric when you talk to the cloud service providers, when you talk to software companies because they are deploying, in many cases, on a multicore environment, and they want to know what does my per-core performance look like.

161. Defendants’ statements made at the UBS Global Technology Conference on November 14, 2017, were false and misleading, and omitted material facts. In truth, the Intel® Xeon® Scalable processors’ architecture was not designed to optimize security as it contained major security flaws. Similarly, the performance of the Intel® Xeon® Scalable processors was overstated, as there are fundamental design flaws in the Xeon Scalable processors that seriously compromise the processors’ security and render them vulnerable

1 to hacking and other exploits. In addition, remedying the defects will significantly impair  
 2 the microprocessors' performance. After the Class Period, Defendants admitted that the  
 3 patches degraded performance. *See* ¶129.

4 **E. November 28, 2017 Credit Suisse**  
 5 **Technology, Media And Telecom Conference**

6 162. On November 28, 2017, Defendant Swan presented at the Credit Suisse  
 7 Technology, Media and Telecom Conference. During the presentation, Swan discussed the  
 8 intersection of client demand for Intel's products versus the performance of those products,  
 9 stating:

10 Question— John William Pitzer: In the core servers Xeon business, how  
 11 important are product cycles? And I probably get 14 or 15 questions a week about  
 12 Purley and sort of how Purley is sort of unfolding and kind of what's the outlook  
 13 there. So can you talk a little bit about product cycle importance in general and  
 specifically how you see Purley rolling out over the next 4 to 6 quarters?

14 Answer – Robert H. Swan: I think I'm going to focus a little bit on the cloud,  
 15 if you don't mind, and if you -- I think -- but I think it applies for enterprise as  
 16 well. ***This is a -- where everyone, all the CIOs, are dealing with this increasing***  
 17 ***demand to be more efficient but to also deal with more cybersecurity threats. The***  
 18 ***demands of their internal customers to get more access to more data, to analyze it***  
 19 ***more effectively are growing and growing and growing.*** And they have -- their  
 20 demands for compute memory and storage are growing like crazy. And in that  
 21 world, you have -- they don't all want to just pay X percent. If they have 30% more  
 22 demand for data, they don't want to pay 30% more for that performance. So what  
 23 they're looking for, CIOs in general, whether they offload to the cloud or perform  
 24 on-premise, they're looking for more performance to deal with the increasing  
 25 challenges that they're facing with. So that more performance comes from just a  
 26 more predictable cadence of new products that deliver higher performance. And so  
 27 that's -- we're trying to continue, much like we are in the client side, just an annual  
 28 rollout of products that can deliver higher performance so they can deal with the  
 increasing demands of what data means for their collective spending envelope. It's  
 very important. Purley is our most recent new product launch, as you know, with  
 dramatically improved performance suite. We launched it in the July time  
 frame. And it's got -- it's just -- it's grown now -- it'll grow over the course of --  
 you got to kind of slot it into their replacement cycles so we don't launch the product  
 and they say, oh, let's go replace everything, but it's been growing over the course  
 of the third quarter. And we expect, as they go through their refresh, the demand  
 for this higher-performance product will continue to grow and will be a source of  
 growth for us in kind of the fourth quarter into 2018.

1           163. These statements were false and misleading, and omitted material facts. In  
2 making these statements, Swan concealed from investors that the Spectre and Meltdown  
3 vulnerabilities exposed users' data to theft. Defendant Swan further misled investors by  
4 concealing that the only permanent solution to address Spectre and Meltdown was a  
5 fundamental redesign of Intel's processors, and that the patches developed to mitigate the  
6 vulnerabilities until a permanent fix could be developed were ineffective and significantly  
7 impaired the processors' performance, especially for heavy workload users like the cloud  
8 clients Swan specifically noted. After the Class Period, Defendants admitted that the  
9 patches degraded performance. Thus, Intel's processors were not meeting its cloud  
10 customers' demands as they contained major security flaws, and remedying the defects will  
11 significantly impair the microprocessors' performance.

12           164. On November 29, 2017, Krzanich sold almost \$40 million of his personal  
13 Intel holdings for a \$25 million profit. As Intel's CEO, Krzanich had access to material  
14 nonpublic information about the existence of Spectre and Meltdown and the adverse  
15 impacts those vulnerabilities and the purported mitigations would have on Intel's  
16 processors. Krzanich owed the Company's shareholders a duty to disclose that information  
17 or abstain from buying or selling Intel stock on the basis of that material nonpublic  
18 information. Had he disclosed the information about Spectre and Meltdown and the  
19 degraded processor performance mitigating those vulnerabilities would cause, the falsity  
20 of Defendants' prior misrepresentations would have been revealed and the artificial  
21 inflation in Intel's stock price would have dissipated.

22           **F. December 5, 2017 Intel Corp At Nasdaq Investor Program**

23           165. On December 5, 2017, Venkata Murthy Renduchintala, Intel's Chief  
24 Engineering Officer and President of Client & Internet of Things Businesses & Systems  
25 Architecture presented the Nasdaq Investor Program. During the conference, Intel touted  
26 its Core platforms' performance, stating, "*If you do a like-by-like performance, from the*  
27 *first product in 14, Broadwell, for example, to the eighth generation Intel device, we've*  
28 *seen an over 30% improvement in the performance of the devices. And that's just a*

1 *testament to how much intra-node benefit there is.*

2 166. This statement was false and misleading, and omitted material facts.  
 3 Specifically, the statement omitted the material facts that (i) the Spectre and Meltdown  
 4 vulnerabilities exposed users' data to theft, (ii) the only permanent solution to address  
 5 Spectre and Meltdown was a fundamental redesign of the Company's processors, and (iii)  
 6 the patches developed to mitigate the vulnerabilities until a permanent fix could be  
 7 implemented were ineffective and significantly impaired the processors' performance,  
 8 especially for heavy workload users. After the Class Period, Defendants admitted that the  
 9 patches degraded performance. *See* ¶129.

#### 10 **G. December 20, 2017 Intel Hardware-Based Security Video**

11 167. On December 20, 2017, Defendants posted a video entitled, "Endpoint  
 12 Security at the Hardware Level" on the Company's website. In the video, Yasser Rasheed,  
 13 Global Director of Business Client Security at Intel, states:

14 Software attack versus software protection, this is a race, a race between the good  
 15 and the bad. There are 4 priorities that IT needs to keep in mind: identity protection,  
 16 data protection, threat detection, and prevention and recovery from breaches; at the  
 17 end of the day end users will always opt for what's simpler and what makes them  
 18 productive and they will deprioritize what makes them more secure. IT needs to  
 19 now make it simpler and easier for end users to be productive and on the back end  
 20 add the right infrastructure for auditability, compliance and so on. Hardware-based  
 21 protection makes it exponentially harder for the attackers to get in. ***We have the  
 ability to protect against identity breaches with multi-factor authentication in the  
 hardware protecting the factors, the policy and the credentials. At Intel we believe  
 we have an opportunity to bring in hardware-based protection in such a way that  
 protects the good people from the bad people.***

22 168. These statements were false and misleading, and omitted material facts. In  
 23 making these statements, Defendants concealed from investors that the Spectre and  
 24 Meltdown vulnerabilities exposed users' data to theft. Defendants further misled investors  
 25 by concealing that the only permanent solution to address Spectre and Meltdown was a  
 26 fundamental redesign of Intel's processors, and that the patches developed to mitigate the  
 27 vulnerabilities until a permanent fix could be developed were ineffective and significantly  
 28 impaired the processors' performance, especially for heavy workload users like the cloud

clients Swan specifically noted. After the Class Period, Defendants admitted that the patches degraded performance.

## **VI. ADDITIONAL ALLEGATIONS OF DEFENDANTS' SCIENTER**

169. Numerous facts in addition to those set forth above give rise to a strong inference that Defendants knew, or were deliberately reckless in not knowing, that their statements about the security and performance of Intel's microprocessors were false and misleading or omitted material facts necessary to make them not misleading when made.

170. *Defendants admit that they learned of the Spectre and Meltdown vulnerabilities in June 2017, yet failed to disclose such information while continuing to promote the performance and security of Intel Processors.* In its letter to Congress and its 2017 Annual Report, Intel disclosed that it was informed of Spectre and Meltdown in June 2017. Defendant Krzanich further admitted during his January 3, 2018 appearance on CNBC that "we" learned of vulnerabilities "a while back" and had been working with the Company's industry partners in an attempt to patch the problem. That same evening, Senior Intel managers Smith, Singhal, and Andy Parker admitted that the Company had been working with industry participants "for months" to try to develop patches to address the vulnerabilities.

171. *Defendant Krzanich's insider sales further support an inference of scienter.* On November 29, 2017, the same day Intel notified its OEM partners for the first time of one of the Spectre vulnerabilities, and a month before the Company admitted the existence of the Spectre and Meltdown flaws, Defendant Krzanich sold 890,000 shares of Intel stock, netting almost \$25 million. The number of shares he sold was more than ten times greater than any other sale in the previous two years. He exercised and sold every exercisable option, even though none were set to expire for at least 14 months. And he sold every share he could while maintaining the minimum shares Intel's bylaws require him to own as CEO. Sanford C. Bernstein & Co. analyst Stacy Rasgon was quoted by

1 *Bloomberg* as saying, “In all the years I’ve been at this and of all the companies I’ve  
2 covered, I can’t recall another massive sale of this scale.”<sup>23</sup>

3 172. *It is absurd to suggest that Defendants were not aware of Spectre and*  
4 *Meltdown because the vulnerabilities affected virtually every Intel microprocessor.*  
5 Given that Intel makes 90% of the world’s computer processors and has a 99% market  
6 share for server processors used by cloud providers and data centers that run the internet,  
7 Spectre and Meltdown constituted unprecedented threats to Intel, its customers, and  
8 computer users worldwide. Virtually all of Intel’s revenues come directly or indirectly  
9 from its sale of processors or related products that are impacted by Spectre and Meltdown.  
10 Thus, the problems that Spectre and Meltdown presented were so prominent it is not  
11 plausible that Krzanich, Swan, Shenoy, and other senior management did not know about  
12 those problems when making false statements about the performance and security of Intel’s  
13 processors.

14 173. *The temporal proximity between Defendants’ false statements and*  
15 *omissions and revelations of the truth supports an inference of scienter.* Just six weeks  
16 after falsely touting the supposedly industry-leading performance and security of its  
17 microprocessors, Intel admitted that it had known for months that those microprocessors  
18 contained major security flaws and that the mitigations for those flaws could negatively  
19 impact performance by 30 percent or more depending on workload. Intel also admitted  
20 that at least in the case of Spectre, the vulnerabilities stemmed from a fundamental element  
21 of the processors’ architecture or design.

22 174. *Defendants took undisclosed steps that show their knowledge of Spectre*  
23 *and Meltdown and ineffective patches.* At the same time Defendants were promoting  
24 superior security and performance, the Company secretly worked to verify the  
25 vulnerabilities and find mitigations, requested extension of the 90-day deadline from  
26

---

27  
28 <sup>23</sup> Julie Verhage, “Bernstein Says Optics on Intel CEO Stock Sale Are ‘Indefensible,’”  
*Bloomberg* (Jan. 10, 2018).

1 Google Ground Zero, and notified select clients of the threats on a confidential basis.

2 **175. *Defendants’ failure to notify US-CERT supports an inference of scienter.***

3 US-CERT disclosure guidelines provide guidance for reporting “incidents” that actually or  
4 imminently jeopardize the integrity and confidentiality of sensitive federal information.  
5 Spectre and Meltdown fall within this definition because they jeopardized the security of  
6 sensitive information contained on government computers, servers and networks running  
7 on Intel processors. Defendants’ failure to follow these guidelines to delay disclosure of  
8 the truth regarding their false statements about the security of Intel processors further  
9 supports an inference of scienter.

10 **176. *The suspicious timing and circumstances of Defendant Krzanich’s***  
11 ***departure from Intel further supports an inference of scienter.*** Not long after Intel  
12 confirmed the existence of additional Spectre and Meltdown vulnerabilities, Krzanich  
13 abruptly left the Company on June 21, 2018. Intel publicly claimed that Krzanich resigned  
14 after the Company learned of a “past consensual relationship” with an Intel employee that  
15 ended before Krzanich became CEO in 2013. Analysts are skeptical of this explanation,  
16 noting that previous CEOs and other executives had similar relationships and suffered no  
17 consequences.

18 **177. *As head of the Data Center Group, Defendant Shenoy was personally***  
19 ***involved in efforts to develop and deploy mitigations to Spectre and Meltdown.***

20 Throughout the Class Period, Defendant Shenoy led the Data Center Group, Intel’s  
21 business segment responsible for the Company’s data-centric businesses, including server,  
22 network, and storage-related product lines. According to the former Senior Product  
23 Manager and Engineer of Manufacturing, discussed above in paragraph 75, as Intel  
24 engineers tested potential mitigations, they would have logged the data and presented their  
25 findings and recommendations to the senior executives in the business units directly  
26 impacted by Spectre and Meltdown. At these “forums,” which the Company referred to as  
27 “war rooms,” participants would discuss potential mitigations and their impacts on  
28 performance. Because the Data Center Group was one of those units directly impacted,

Defendant Shenoy, as head of the Data Center Group, would have participated in those discussions and would have made the “final call” on which mitigations to deploy. Shenoy and other senior business leaders in turn would provide Krzanich, Swan and other corporate executives with weekly or bi-weekly reports. The former security engineer cited in paragraph 74 above confirms that the head of the business units impacted by Spectre and Meltdown would have approved the disclosure plan and mitigations.

## **VII. LOSS CAUSATION**

178. Defendants’ materially false and misleading statements and omissions artificially inflated the price of Intel common stock before and during the Class Period and maintained inflation in the stock price. A series of partial disclosures revealed the relevant truth and removed the artificial inflation from the stock price.

179. On January 2, 2018, after the market closed, British technology website *The Register* reported that effectively every Intel processor currently in use suffers from a major design flaw, now called “Meltdown,” and that to fix the flaw, providers of major operating systems are instituting software patches to isolate the kernel memory, but these updates may handicap the performance of Intel chips by up to 30%.

180. This partial disclosure caused Intel’s stock price to decline. On January 3, 2018, the share price fell \$1.59 per share, or approximately 3%.

181. On January 3, 2018, after trading hours, Google Project Zero and other researchers published their findings, announcing that Intel and several other manufacturers’ processors suffered from a similar defect named “Spectre.” That same day, after trading hours, Intel issued a press release and held a special investor call acknowledging the security vulnerabilities, but stating that potential performance slowdowns had been exaggerated.

182. These partial disclosures caused Intel’s stock price to decline. On January 4, 2018, the share price fell \$0.83, or approximately 2%.

183. On January 8, 2018, after trading hours, news outlets reported that Krzanich’s comments at CES 2018 indicated that fixes for Spectre and Meltdown would

1 cause a bigger slowdown than Defendants had previously suggested, and that the problem  
 2 may be more pervasive than Defendants originally represented. The following day, on  
 3 January 9, 2018, news sources reported that Intel met with PC vendors at the end of 2017  
 4 to discuss resolutions for its processors' security issues, but failed to come to a resolution,  
 5 and that these PC vendors believed the effect of the security flaws on PC demand would  
 6 manifest during the first half of 2018. In addition, on January 9, 2018, Microsoft released  
 7 new data about the impact of fixes to the security vulnerabilities, and revealed that such  
 8 fixes may "significantly" slow down the performance of certain servers and some personal  
 9 computers.

10 184. These partial disclosures caused Intel's stock price to decline. On January 9,  
 11 2018, shares of Intel fell \$1.12, or 2.5%.

12 185. On January 10, 2018, before trading hours, *Forbes* reported the results from  
 13 independent tests carried out by a security researcher showing that heavy processor  
 14 workloads could see a "significant impact." Other news sources similarly reported that  
 15 because of the security vulnerabilities, Intel's data center customers, whose computers run  
 16 cloud networks, were exploring using microprocessors from Intel's rivals to build new  
 17 infrastructure.

18 186. These partial disclosures caused Intel's stock price to decline. On January  
 19 10, 2018, shares of Intel fell \$1.12, or 2.6%.

## 20 **VIII. PRESUMPTION OF RELIANCE**

21 187. At all relevant times, the market for Intel's common stock was efficient for  
 22 the following reasons, among others:

- 23 (a) Intel's stock met the requirements for listing, and was listed and actively  
 24 traded on the Nasdaq Stock Market, a highly efficient and automated market;
- 25 (b) As a regulated issuer, Intel filed periodic reports with the SEC and the  
 26 Nasdaq Stock Market;
- 27 (c) Intel regularly communicated with public investors via established market  
 28 communication mechanisms, including through regular disseminations of press  
 releases on the national circuits of major newswire services and through other wide-

1 ranging public disclosures, such as communications with the financial press and  
2 other similar reporting services; and

3 (d) Intel was followed by numerous securities analysts employed by major  
4 brokerage firms who wrote reports which were distributed to those brokerage firms'  
5 sales force and certain customers. Each of these reports was publicly available and  
6 entered the public market place.

7 188. As a result of the foregoing, the market for Intel's common stock reasonably  
8 and promptly digested current information regarding Intel from all publicly available  
9 sources and reflected such information in the price of Intel's common stock. All purchasers  
10 of Intel's common stock during the Class Period suffered similar injury through their  
11 purchase of Intel's common stock at artificially inflated prices, and a presumption of  
12 reliance applies.

13 189. A Class-wide presumption of reliance also is appropriate under the United  
14 States Supreme Court holding in *Affiliated Ute Citizens of Utah v. United States*, 406 U.S.  
15 128 (1972), because the claims asserted herein against Defendants are predicated on  
16 omissions of material fact for which there is a duty to disclose.

## 17 **IX. DEFENDANTS' DUTY TO DISCLOSE**

18 190. As described above, Defendants Intel, Krzanich, Swan, and Shenoy had a  
19 duty to disclose the truth about the performance and security of Intel's processors when  
20 speaking on that subject. Before and throughout the Class Period, Defendants made a  
21 series of statements regarding the security and performance of Intel's processors. Having  
22 chosen to speak positively about the Company's processors, Defendants had a duty to  
23 disclose material facts necessary to make their statements not misleading. By omitting  
24 information about the Spectre and Meltdown security vulnerabilities and the degraded  
25 performance the fixes would cause when making their positive statements, Defendants  
26 created an impression of a state of affairs that differed in a material way from the one that  
27 actually existed.

28 191. Moreover, as Intel's CEO, Defendant Krzanich had access to material  
nonpublic information about the security and performance of the Company's processors.

1 Krzanich owed the Company's shareholders a duty to disclose or abstain from buying or  
2 selling Intel stock on the basis of that material nonpublic information. Thus, before selling  
3 his Intel stock on November 29, 2017, Krzanich had an affirmative duty to disclose to  
4 investors information known to him about the Spectre and Meltdown security  
5 vulnerabilities and the degraded processor performance mitigating those vulnerabilities  
6 would cause.

7 **X. INAPPLICABILITY OF THE STATUTORY SAFE**  
8 **HARBOR AND BESPEAKS CAUTION DOCTRINE**

9 192. The statutory safe harbor or bespeaks caution doctrine applicable to forward-  
10 looking statements under certain circumstances does not apply to any of the false and  
11 misleading statements pleaded in this Complaint. None of the statements complained of  
12 herein was a forward-looking statement. Rather, they were historical statements or  
13 statements of purportedly current facts and conditions at the time the statements were  
14 made.

15 193. To the extent that any of the false and misleading statements alleged herein  
16 can be construed as forward-looking, those statements were not accompanied by  
17 meaningful cautionary language identifying important facts that could cause actual results  
18 to differ materially from those in the statements. Then-existing facts contradicted  
19 Defendants' statements regarding the security and performance of Intel's processors.  
20 Given the then-existing facts contradicting Defendants' statements, any generalized risk  
21 disclosures made by the Company were not sufficient to insulate Defendants from liability  
22 for their materially false and misleading statements and omissions.

23 194. To the extent that the statutory safe harbor does apply to any forward-looking  
24 statements pleaded herein, Defendants are liable for those false forward-looking statements  
25 because at the time each of those statements was made, the particular speaker knew that  
26 the particular forward-looking statement was false, and the false forward-looking statement  
27 was authorized and approved by an executive officer of Intel who knew that the statement  
28 was false when made.

1 **XI. CLASS ACTION ALLEGATIONS**

2 195. Lead Plaintiff brings this action as a class action under Rule 23 of the Federal  
3 Rules of Civil Procedure on behalf of all persons who purchased the common stock of Intel  
4 between October 27, 2017 and January 9, 2018.

5 196. Excluded from the Class are (i) Defendants; (ii) members of the immediate  
6 family of each Individual Defendant; (iii) any person who was an officer or director of  
7 Intel; (iv) any firm or entity in which any Defendant has or had a controlling interest; (v)  
8 any person who participated in the wrongdoing alleged; (vi) Defendants' liability insurance  
9 carriers; (vii) any affiliates, parents, or subsidiaries of Intel; (viii) all Intel plans that are  
10 covered by ERISA; and (ix) the legal representatives, agents, affiliates, heirs, beneficiaries,  
11 successors-in-interest, or assigns of any excluded person or entity, in their respective  
12 capacity as such.

13 197. The members of the Class are so numerous that joinder of all members is  
14 impracticable. Throughout the Class Period, Intel shares were actively traded on the  
15 Nasdaq Stock Market. As of July 9, 2018, there were approximately 4.68 billion shares of  
16 Intel stock outstanding. While the exact number of Class members is unknown to Lead  
17 Plaintiff at this time and can only be ascertained through appropriate discovery, Lead  
18 Plaintiff believes that there are thousands of members of the proposed Class. Class  
19 members who purchased Intel common stock may be identified from records maintained  
20 by Intel or its transfer agent(s), and may be notified of this class action using a form of  
21 notice similar to that customarily used in securities class actions.

22 198. Lead Plaintiff's claims are typical of Class members' claims, as all members  
23 of the Class were similarly affected by Defendants' wrongful conduct in violation of federal  
24 laws as complained of herein.

25 199. Lead Plaintiff will fairly and adequately protect Class members' interests and  
26 have retained competent counsel experienced in class actions and securities litigation.

27 200. Common questions of law and fact exist as to all Class members and  
28 predominate over any questions solely affecting individual Class members. Among the

1 questions of fact and law common to the Class are:

- 2 (a) whether the federal securities laws were violated by Defendants' acts
- 3 as alleged herein;
- 4 (b) whether Defendants made statements to the investing public during the
- 5 Class Period that were false, misleading or omitted material facts;
- 6 (c) whether Defendants acted with scienter; and
- 7 (d) the proper way to measure damages.

8 201. A class action is superior to all other available methods for the fair and  
 9 efficient adjudication of this action because joinder of all Class members is impracticable.  
 10 Additionally, the damage suffered by some individual Class members may be relatively  
 11 small so that the burden and expense of individual litigation make it impossible for such  
 12 members to individually redress the wrong done to them. There will be no difficulty in the  
 13 management of this action as a class action.

## 14 **XII. CLAIMS FOR RELIEF**

### 15 **COUNT I**

#### 16 **For Violations Of Section 10(b) Of** 17 **The Exchange Act And SEC Rule 10b-5** 18 **Promulgated Thereunder (Against All Defendants)**

19 202. Lead Plaintiff repeats and realleges each and every allegation contained  
 20 above as if fully set forth herein.

21 203. This Count is asserted on behalf of all members of the Class against  
 22 Defendants Intel, Krzanich, Swan and Shenoy for violations of Section 10(b) of the  
 23 Exchange Act, 15 U.S.C. § 78j(b) and Rule 10b-5 promulgated thereunder, 17 C.F.R. §  
 24 240.10b-5.

25 204. During the Class Period, Defendants disseminated or approved the false  
 26 statements specified above, which they knew were, or they deliberately disregarded as,  
 27 misleading in that they contained misrepresentations and failed to disclose material facts  
 28 necessary in order to make the statements made, in light of the circumstances under which

1 they were made, not misleading.

2       205. Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 in  
3 that they: (a) employed devices, schemes, and artifices to defraud; (b) made untrue  
4 statements of material facts or omitted to state material facts necessary in order to make  
5 the statements made, in light of the circumstances under which they were made, not  
6 misleading; and/or (c) engaged in acts, practices, and a course of business that operated as  
7 a fraud or deceit upon Lead Plaintiff and others similarly situated in connection with their  
8 purchases of Intel common stock during the Class Period.

9       206. Defendants, individually and in concert, directly and indirectly, by the use of  
10 means or instrumentalities of interstate commerce and/or of the mails, engaged and  
11 participated in a continuous course of conduct that operated as a fraud and deceit upon  
12 Lead Plaintiff and the Class; made various untrue and/or misleading statements of material  
13 facts and omitted to state material facts necessary in order to make the statements made, in  
14 light of the circumstances under which they were made, not misleading; made the above  
15 statements intentionally or with a deliberately reckless disregard for the truth; and  
16 employed devices and artifices to defraud in connection with the purchase and sale of Intel  
17 common stock, which were intended to, and did: (a) deceive the investing public, including  
18 Lead Plaintiff and the Class, regarding, among other things, the security and performance  
19 of Intel's processors; (b) artificially inflate and maintain the market price of Intel common  
20 stock; and (c) cause Lead Plaintiff and other members of the Class to purchase Intel  
21 common stock at artificially inflated prices and suffer losses when the true facts became  
22 known.

23       207. Defendants Intel, Krzanich, Swan, and Shenoy are liable for all materially  
24 false and misleading statements made during the Class Period, as alleged above.

25       208. As described above, Defendants acted with scienter throughout the Class  
26 Period, in that they acted either with intent to deceive, manipulate, or defraud, or with  
27 deliberate recklessness. The misrepresentations and omissions of material facts set forth  
28 herein, which presented a danger of misleading buyers or sellers of Intel stock, were either

1 known to the Defendants or were so obvious that the Defendants should have been aware  
2 of them.

3 209. Lead Plaintiff and the Class have suffered damages in that, in reliance on the  
4 integrity of the market, they paid artificially inflated prices for Intel common stock, which  
5 inflation was removed from its price when the true facts became known. Lead Plaintiff  
6 and the Class would not have purchased Intel common stock at the prices they paid, or at  
7 all, if they had been aware that the market price had been artificially and falsely inflated  
8 by these Defendants' misleading statements.

9 210. As a direct and proximate result of these Defendants' wrongful conduct, Lead  
10 Plaintiff and the other members of the Class suffered damages attributable to the material  
11 misstatements and omissions alleged herein in connection with their purchases of Intel  
12 common stock during the Class Period.

## 13 **COUNT II**

### 14 **For Violation Of Section 20(a) Of The Exchange** 15 **Act Against Individual Defendants Krzanich, Swan And Shenoy**

16 211. Lead Plaintiff repeats and realleges each and every allegation contained  
17 above as if fully set forth herein.

18 212. This Count is asserted on behalf of all members of the Class against  
19 Individual Defendants Krzanich, Swan and Shenoy for violations of Section 20(a) of the  
20 Exchange Act, 15 U.S.C. § 78t(a).

21 213. During their tenures as officers and/or directors of Intel, each of these  
22 Individual Defendants was a controlling person of the Company within the meaning of  
23 Section 20(a) of the Exchange Act. *See ¶¶19-21.* By reason of their positions of control  
24 and authority as officers and/or directors of Intel, these Individual Defendants had the  
25 power and authority to direct the management and activities of the Company and its  
26 employees, and to cause the Company to engage in the wrongful conduct complained of  
27 herein. These Individual Defendants were able to and did control, directly and indirectly,  
28 the content of the public statements made by Intel during the Class Period, including its

1 materially misleading financial statements, thereby causing the dissemination of the false  
2 and misleading statements and omissions of material facts as alleged herein.

3       214. In their capacities as senior corporate officers of the Company, and as more  
4 fully described above in ¶¶19-21, the Individual Defendants had direct involvement in the  
5 day-to-day operations of the Company, in reviewing and managing its regulatory and legal  
6 compliance, and in its reporting functions. Individual Defendants signed the Company's  
7 SEC filings during the Class Period, and/or were directly involved in providing false  
8 information and certifying and approving the false statements disseminated by Intel during  
9 the Class Period. As a result of the foregoing, the Individual Defendants, as a group and  
10 individually, were controlling persons of Intel within the meaning of Section 20(a) of the  
11 Exchange Act.

12       215. As set forth above, Intel violated Section 10(b) of the Exchange Act by its  
13 acts and omissions as alleged in this Complaint.

14       216. By virtue of their positions as controlling persons of Intel and as a result of  
15 their own aforementioned conduct, the Individual Defendants are liable pursuant to Section  
16 20(a) of the Exchange Act, jointly and severally with, and to the same extent as, the  
17 Company is liable under Section 10(b) of the Exchange Act and Rule 10b-5 promulgated  
18 thereunder, to Lead Plaintiff and the other members of the Class who purchased or  
19 otherwise acquired Intel common stock. As detailed above, during the respective times  
20 these Individual Defendants served as officers and/or directors of Intel, each of these  
21 Individual Defendants was culpable for the material misstatements and omissions made by  
22 Intel.

23       217. As a direct and proximate result of these Individual Defendants' conduct,  
24 Lead Plaintiff and the other members of the Class suffered damages in connection with  
25 their purchase or acquisition of Intel common stock.

26 **XIII. PRAYER FOR RELIEF**

27       218. WHEREFORE, Lead Plaintiff prays for relief and judgment as follows:

28           (a) Declaring the action to be a proper class action pursuant to Rule 23(a)

and (b)(3) of the Federal Rules of Civil Procedure on behalf of the Class defined herein;

(b) Awarding all damages and other remedies available under the Exchange Act in favor of Lead Plaintiff and all members of the Class against Defendants in an amount to be proven at trial, including interest thereon;

(c) Awarding Lead Plaintiff and the Class their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

(d) Such other and further relief as the Court may deem just and proper.

#### **XIV. JURY DEMAND**

Lead Plaintiff demands a trial by jury.

Dated: July 10, 2018

Respectfully submitted,

BERNSTEIN LITOWITZ BERGER  
& GROSSMANN LLP

/s/ David R. Stickney  
DAVID R. STICKNEY

David R. Stickney  
Richard D. Gluck  
Lucas E. Gilmore  
12481 High Bluff Drive, Suite 300  
San Diego, CA 92130  
Tel: (858) 793-0070  
Fax: (858) 793-0323  
Email: [davids@blbglaw.com](mailto:davids@blbglaw.com)  
Email: [rich.gluck@blbglaw.com](mailto:rich.gluck@blbglaw.com)  
Email: [lucas.gilmore@blbglaw.com](mailto:lucas.gilmore@blbglaw.com)

-and-

AVI JOSEFSON  
([avi@blbglaw.com](mailto:avi@blbglaw.com))  
1251 Avenue of the Americas  
New York, NY 10020  
Tel: (212) 554-1400  
Fax: (212) 554-1444  
Email: [avi@blbglaw.com](mailto:avi@blbglaw.com)

*Attorneys for Lead Plaintiff Louisiana  
Sheriffs' Pension & Relief Fund and  
Lead Counsel for the Class*

**CERTIFICATION PURSUANT TO  
THE FEDERAL SECURITIES LAWS**

I, Osey McGee, on behalf of Louisiana Sheriffs' Pension & Relief Fund ("Louisiana Sheriffs"), hereby certify, as to the claims asserted under the federal securities laws, that:

1. I am the Executive Director of Louisiana Sheriffs. I have reviewed the consolidated complaint with the Fund's legal counsel, and based on the legal counsel's knowledge and advice, authorize its filing.
2. Louisiana Sheriffs did not purchase the securities that are the subject of this action at the direction of counsel or in order to participate in any action arising under the federal securities laws.
3. The Court appointed Louisiana Sheriffs as Lead Plaintiff on May 29, 2018. Louisiana Sheriffs is willing to serve as a representative party on behalf of the Class, including providing testimony at deposition and trial, if necessary.
4. Louisiana Sheriffs' transactions in the Intel Corporation securities that are the subject of this action are set forth in the chart attached hereto.
5. Louisiana Sheriffs has sought to serve and was appointed as a lead plaintiff and representative party on behalf of a class in the following actions under the federal securities laws filed during the three-year period preceding the date of this Certification:

*Sanchez v. Centene Corp.*,  
No. 17-cv-806 (E.D. Mo.)  
*Tung v. Bristol-Myers Squibb Co.*,  
No. 18-cv-1611 (S.D.N.Y.)


6. Louisiana Sheriffs has sought to serve as a lead plaintiff and representative party on behalf of a class in the following actions under the federal securities laws filed during the three-year period preceding the date of this Certification, but either withdrew its motions for lead plaintiff or was not appointed lead plaintiff:

*Washtenaw County Employees' Retirement System v. Walgreen Co.*,  
No. 15-cv-3187 (N.D. Ill.)  
*In re Eaton Corporation Securities Litigation*,  
No. 16-cv-5894 (S.D.N.Y.)

7. Louisiana Sheriffs will not accept any payment for serving as a representative party on behalf of the Class beyond Louisiana Sheriffs' pro rata share of any recovery, except such reasonable costs and expenses (including lost wages) directly relating to the representation of the Class, as ordered or approved by the Court.

Louisiana Sheriffs has relied on the research and analysis of the consolidated complaint provided by legal counsel Bernstein Litowitz Berger & Grossmann LLP. The undersigned declares that the statements made and information provided are, to the best of his knowledge, true and correct.

Executed this 10<sup>th</sup> day of July, 2018.

  
\_\_\_\_\_  
Osey McGee  
Executive Director  
*Louisiana Sheriffs' Pension & Relief Fund*

**Louisiana Sheriffs' Pension & Relief Fund**  
**Transactions in Intel Corporation**

<u>Transaction</u>	<u>Date</u>	<u>Shares</u>	<u>Price</u>
Purchase	11/10/2017	18,973	45.6095
Purchase	11/10/2017	11,747	45.6541
Purchase	11/13/2017	30,572	45.7432
Sale	11/28/2017	(8,350)	44.5221
Sale	11/28/2017	(8,105)	44.5082
Sale	11/28/2017	(12,792)	44.5255
Sale	01/08/2018	(12,916)	44.6367
Sale	01/08/2018	(19,129)	44.6367